

HERRERA PURDY LLP  
Shawn M. Kennedy (SBN 218472)  
*skennedy@herrerapurdy.com*  
Andrew M. Purdy (SBN 261912)  
*apurdy@herrerapurdy.com*  
Bret D. Hembd (SBN 272826)  
*bhembd@herrerapurdy.com*  
4590 MacArthur Blvd., Suite 500  
Newport Beach, CA 92660  
Tel: (949) 936-0900  
Fax: (855) 969-2050

HERRERA PURDY LLP  
Nicomedes Sy Herrera (SBN 275332)  
*nherrera@herrerapurdy.com*  
Laura E. Seidl (SBN 269891)  
*lseidl@herrerapurdy.com*  
1300 Clay Street, Suite 600  
Oakland, CA 94612  
Tel: (510) 422-4700  
Fax: (855) 969-2050

LIEFF CABRASER HEIMANN &  
BERNSTEIN, LLP  
Rachel Geman (*Pro Hac Vice*)  
*rgeman@lchb.com*  
250 Hudson Street, 8th Floor  
New York, NY 10013-1413  
Tel: (212) 355-9500  
Fax: (212) 355-9592

LIEFF CABRASER HEIMANN &  
BERNSTEIN, LLP  
Michael W. Sobol (SBN 194857)  
*msobol@lchb.com*  
Melissa Gardner (SBN 289096)  
*mgardner@lchb.com*  
275 Battery Street, 29<sup>th</sup> Floor  
San Francisco, CA 94111-3339  
Tel: (415) 956-1000  
Fax: (415) 956-1008

BURNS CHAREST LLP  
Warren T. Burns (*Pro Hac Vice*)  
*wburns@burnscharest.com*  
Russell Herman (*Pro Hac Vice*)  
*rherman@burnscharest.com*  
900 Jackson Street, Suite 500  
Dallas, TX 75202  
Tel: (469) 904-4550  
Fax: (469) 444-5002

BURNS CHAREST LLP  
Christopher J. Cormier (*Pro Hac Vice*)  
*ccormier@burnscharest.com*  
4725 Wisconsin Avenue, NW, Suite 200  
Washington, DC 20016  
Tel: (202) 577-3977  
Fax: (469) 444-5002

*Interim Co-Lead Class Counsel*

[Additional counsel on signature page]

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
OAKLAND DIVISION

IN RE PLAID INC. PRIVACY  
LITIGATION

Master Docket No.: 4:20-cv-03056

**CONSOLIDATED AMENDED CLASS  
ACTION COMPLAINT FOR DAMAGES  
AND DECLARATORY AND EQUITABLE  
RELIEF**

THIS DOCUMENT RELATES TO:  
ALL ACTIONS

**DEMAND FOR JURY TRIAL**

## TABLE OF CONTENTS

		<u>Page</u>
1		
2		
3	I. INTRODUCTION .....	1
4	II. JURISDICTION AND VENUE .....	3
5	III. INTRADISTRICT ASSIGNMENT .....	3
6	IV. THE PARTIES .....	4
7	V. FACTUAL BACKGROUND .....	5
8	A. Background of Plaid and the Participating Apps .....	5
9	B. Plaid Deceptively Obtains Bank Account Credentials from App Users .....	7
10	C. Plaid Leverages Credentials to Collect Valuable Data on a Massive Scale .....	14
11	D. Plaid Sells and Otherwise Exploits the Unlawfully-Obtained Private Data .....	18
12	E. Plaid and Its Fintech Clients Conceal Plaid's Conduct from Consumers .....	20
13	1. Venmo: An Illustrative Example .....	20
14	2. Recent Changes to Venmo's Software .....	23
15	3. The Deceptive Nature of Plaid's Software .....	26
16	F. Plaid's Harm to Consumers is Recognized by Banks and Industry Groups .....	29
17	G. Plaid Knowingly Violates Established Industry Standards and Obligations .....	33
18	1. The GLBA Standards .....	34
19	2. Plaid's Acknowledgement of Its Disclosure Obligations .....	36
20	3. Violations of GLBA Standards in Plaid's Privacy Policy .....	38
21	4. Violations of CalFIPA and CalOPPA Standards in Plaid's Privacy Policy .....	40
22	VI. INJURY AND DAMAGES TO THE CLASS .....	41
23	A. The Named Plaintiffs' Experiences .....	41
24	B. Injuries from Invasions of Privacy and Dignitary Violations .....	62
25	C. Economic Damages .....	65
26	1. Loss of Valuable Indemnification Rights .....	65
27	2. Diminished Value of Rights to Protection of Data .....	68
28	3. Loss of Control Over Valuable Property .....	68
	4. Increased Risk of Identity Theft and Fraud .....	69
	VII. CHOICE OF LAW .....	70
	VIII. TOLLING, CONCEALMENT, AND ESTOPPEL .....	70

**TABLE OF CONTENTS**

(continued)

	<b><u>Page</u></b>
IX. CLASS ACTION ALLEGATIONS .....	71
X. CLAIMS FOR RELIEF .....	76
PRAYER FOR RELIEF .....	104
DEMAND FOR JURY TRIAL .....	105

1 Plaintiffs, individually and as representatives of classes of similarly situated persons, by  
2 their undersigned counsel, allege as follows against Defendant Plaid Inc. ("Plaid"):

3 **I. INTRODUCTION**

4 1. The typical consumer knows nothing about Plaid. That is by design, because Plaid  
5 intentionally operates as a behind-the-scenes financial technology company. Plaid, however,  
6 knows a great deal about the typical consumer. For millions of unsuspecting app users, Plaid  
7 knows every dollar they deposit, withdraw, charge to a credit card, or put away for retirement,  
8 within hours after these the transactions occur. Plaid has at its fingertips information on their  
9 medical bills, mortgage loans, and student debt. With no consent or justification, Plaid tracks  
10 these consumers' every financial move, using improperly-obtained usernames and passwords to  
11 harvest financial information for its sprawling database, multiple times a day.

12 2. Plaid is not a bank. Plaid is not a company that consumers knowingly contact or  
13 entrust with their deeply private information. Yet Plaid has quietly built one of the most  
14 successful tech startups in the financial technology, or "fintech," industry by acquiring vast troves  
15 of information about consumers' private financial lives. This information is among the most  
16 valuable and sensitive of all consumer data. Among other insights, it tells the story of consumers'  
17 creditworthiness and their personal responsibilities, interests, and priorities. The common law of  
18 privacy, as well as multiple federal and state statutes, safeguard such information. Plaid has  
19 repeatedly flouted these laws and norms.

20 3. Specifically, Plaid gathers all this data through software embedded in widely-used  
21 fintech apps such as Venmo, Coinbase, Square's "Cash App," and Stripe. Plaid's stated mission is  
22 to make it "easy" for consumers to "connect" their bank accounts to these fintech apps. But Plaid  
23 conceals its conduct and true intentions from consumers. Indeed, Plaid for years has exploited its  
24 position as middleman to acquire app users' banking login credentials and then use those  
25 credentials to harvest detailed transaction histories and other financial data, all without consent.  
26 Plaid has perpetrated this scheme to assemble what it touts as "one of the largest transactional  
27 data sets in the world."  
28

1           4.       First, Plaid induces consumers to hand over their private bank login credentials to  
2 *Plaid* by making it appear those credentials are being communicated directly to consumers'  
3 *banks*. Consumers are informed the connection is “private” and “secure,” and their banking  
4 credentials will “never be made accessible” to the app. They are then directed to a login screen  
5 that looks like it is coming from their bank, complete with the bank’s logo and branding. In  
6 reality, however, though Plaid does not disclose this, the login screen is created by, controlled by,  
7 and connected to Plaid. Plaid executives have acknowledged this process was “optimized” to  
8 increase “user conversions”—in other words, to provide a false sense of comfort to consumers by  
9 concealing Plaid’s role as an unaffiliated third party.

10           5.       Second, Plaid uses consumers’ login credentials to obtain *direct and full* access to  
11 consumers’ personal financial banking information for Plaid’s own commercial purposes wholly  
12 unrelated to consumers’ use of the apps. For each consumer, Plaid downloads years’ worth of  
13 transaction history for *every single account* they have connected to that bank (such as checking,  
14 savings, credit card, and brokerage accounts), regardless of whether the data in any of the  
15 accounts bears any relationship to the app for which the consumer signed up. Thus, a consumer  
16 who makes a single mobile payment on an app from a checking account unwittingly gives Plaid  
17 years’ worth of private, granular financial information from every account the consumer  
18 maintains with the bank, including accounts maintained for others such as relatives and children.  
19 To date, Plaid has amassed this trove of data from over **200 million** distinct financial accounts.

20           6.       Plaid exploits its ill-gotten information in a variety of ways, including marketing  
21 the data to its app customers, analyzing the data to derive insights into consumer behavior, and,  
22 most recently, selling its collection of data to Visa as part of a multi-billion dollar acquisition.  
23 Plaid has unfairly benefited from the personal information of millions of Americans and  
24 wrongfully intruded upon their private financial affairs.

25           7.       Accordingly, Plaintiffs, on behalf of themselves and similarly situated consumers,  
26 bring this action to seek declaratory and injunctive relief requiring Plaid to cease its misconduct,  
27 purge the data it has unlawfully collected, notify consumers of its misconduct, and inform  
28 consumers of the steps they can take to protect themselves from further invasions. Plaintiffs also

1 seek economic redress for Plaid's violations of consumers' dignitary rights, privacy, and well-  
2 being caused by Plaid's unethical and undisclosed invasions into their financial affairs.

## 3 **II. JURISDICTION AND VENUE**

4 8. Pursuant to 28 U.S.C. § 1331, this Court has original subject matter jurisdiction  
5 over the claims that arise under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the  
6 Stored Communications Act, 18 U.S.C. § 2701.

7 9. This Court also has supplemental jurisdiction over the asserted state law claims  
8 pursuant to 28 U.S.C. § 1367.

9 10. This Court has diversity jurisdiction pursuant to 28 U.S.C. § 1332(d) under the  
10 Class Action Fairness Act because the amount in controversy exceeds \$5,000,000, exclusive of  
11 interest and costs, and at least one Class member is a citizen of a state different from Plaid.

12 11. This Court has personal jurisdiction over Defendant because Plaid has conducted  
13 business in the State of California, and because Plaid has committed acts and omissions  
14 complained of herein in the State of California.

15 12. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Plaid does  
16 business in and is subject to personal jurisdiction in this District. Venue is also proper because a  
17 substantial part of the events or omissions giving rise to the claims occurred in or emanated from  
18 this District.

## 19 **III. INTRADISTRICT ASSIGNMENT**

20 13. Pursuant to Civil L.R. 3-2(c) and (d), assignment to the Oakland Division of this  
21 District is proper because all civil actions which arise in San Francisco county shall be assigned  
22 to the San Francisco Division or the Oakland Division, and a substantial part of the conduct  
23 which gives rise to Plaintiffs' claims occurred in the City and County of San Francisco. Plaid  
24 markets and deploys its products throughout the United States, including in San Francisco.  
25 Additionally, Plaid is headquartered in San Francisco and developed the software at issue in this  
26 action in this District.

1 **IV. THE PARTIES**

2 14. **Plaintiff Caroline Anderson** is a citizen and resident of the State of New  
3 Hampshire.

4 15. **Plaintiff James Cottle** is a citizen and resident of the State of California.

5 16. **Plaintiff Rachel Curtis** is a citizen and resident of the State of Florida.

6 17. **Plaintiff David Evans** is a citizen and resident of the State of California.

7 18. **Plaintiff Logan Mitchell** is a citizen and resident of the State of California.

8 19. **Plaintiff Alexis Mullen** is a citizen and resident of the Commonwealth of  
9 Pennsylvania.

10 20. **Plaintiff Jordan Sacks** is a citizen and resident of the District of Columbia.

11 21. **Plaintiff Frederick Schoeneman** is a citizen and resident of the State of  
12 California.

13 22. **Plaintiff Gabriel Sotelo** is a citizen and resident of the State of California.

14 23. **Plaintiff Jeffrey Umali** is a citizen and resident of the State of California.

15 24. **Plaintiff Nicholas Yeomelakis** is a citizen and resident of the Commonwealth of  
16 Massachusetts

17 25. **Defendant Plaid Inc.** is a financial technology company that describes its  
18 business as building the technical infrastructure that connects consumers, financial institutions,  
19 and fintech developers. In addition, Plaid says that it delivers “key insights” on top of data access  
20 through its suite of analytics products.<sup>1</sup> Plaid is a Delaware corporation with its principal place of  
21 business at 85 Second Street, Suite 400, San Francisco, California 94105. On January 13, 2020,  
22 Plaid announced that it had signed a definitive agreement to be acquired by Visa for \$5.3 billion  
23 dollars.<sup>2</sup> The deal is expected to close soon, pending regulatory review and closing conditions.<sup>3</sup>

24  
25  
26 <sup>1</sup> See <https://plaid.com/company/>.

27 <sup>2</sup> See Jan. 13, 2020 Press Release: *Visa To Acquire Plaid*, <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.16856.html>.

28 <sup>3</sup> See <https://www.wsj.com/articles/visas-bet-on-plaid-is-costly-but-necessary-11579001400>;  
<https://invezz.com/news/2020/01/14/payments-giant-visa-acquiring-crypto-serving-fintech-firm-plaid/>.

1 **V. FACTUAL BACKGROUND**

2 **A. Background of Plaid and the Participating Apps**

3 26. Plaid was founded in 2012 by Zach Perret and William Hockey. The two initially  
4 founded Plaid with the intention of building a consumer-facing fintech app. By early 2013,  
5 however, they pivoted to building a behind-the-scenes data aggregator and data brokerage  
6 operation: the fintech infrastructure product known as Plaid.<sup>4</sup>

7 27. Although Plaid's co-founders conceal Plaid's true nature and intentions from  
8 consumers, they evidenced their actual intentions within the financial technology industry early in  
9 the company's existence while they were still formulating their strategy. As early as February  
10 2013, when Perret and Hockey introduced Plaid at the insular "NYC Data Business Meetup," the  
11 co-founders made clear that Plaid's true purpose is to monetize consumer transactional and other  
12 banking data. Collecting and aggregating data from financial institutions was merely the "table  
13 stakes," as Plaid's real goal was to "resolve data and make that something interesting." They  
14 emphasized the "immense" amount of consumer spending data the company could collect from  
15 banks—going back up to five years—and the "awesome" things Plaid could do with the data. At  
16 that time, they reported that Plaid could collect detailed information regarding 3,700 transactions  
17 (covering about \$190,000 of spending) for the average consumer, along with 1,750 unique  
18 geolocations to which the transactions were mapped. Perret explained that this broad and  
19 extensive data collection sets Plaid apart from other apps in the "tried and true" bank-connection  
20 and data-aggregation process.<sup>5</sup>

21 28. Further, in a February 2013 thread on Y Combinator's Hacker News forum,  
22 Hockey stated that Plaid's software made it simple for an application to link with consumer credit  
23 and debit card spending data—a convenience that would eventually rocket Plaid into use by more  
24 than 2,000 applications today. Hockey also stated (but would keep hidden from consumers) that  
25

26 <sup>4</sup> See Apr. 13, 2018 Forbes Article: *Fintech's Happy Plumbers*, <https://www.forbes.com/plaid-fintech/#3c71271167f9>; 5/13/19 interview with Zach Perret at Data Driven NYC event,  
27 <https://www.youtube.com/watch?v=sgnCs34mopw>.

28 <sup>5</sup> See Feb. 2013 presentation by Zach Perret and William Hockey at NYC Data Business Meetup  
at 2:28 to 7:52, [https://www.youtube.com/watch?v=\\_I8DRbFmLKM](https://www.youtube.com/watch?v=_I8DRbFmLKM).



1 in the process of providing that connection, Plaid was “generating one of the largest transactional  
 2 data sets in the world, and using machine learning and statistical analysis to draw insights about  
 3 how consumers spend their time, money, and attention.”<sup>6</sup> Similarly, in a different thread on the  
 4 same forum a month later, Perret stated that Plaid was “building the missing API [Application  
 5 Programming Interface]<sup>7</sup> for Spending Data,” and that in the process, Plaid was “generating one  
 6 of the largest transactional data sets in the world, and using machine learning to draw insights  
 7 about how consumers spend their time, money, and attention.”<sup>8</sup>

8 29. Even Plaid’s company name is a hidden tribute to its true purpose (contrary to its  
 9 public image as an infrastructure tool, to the extent the public learns of Plaid at all), which is  
 10 monetizing consumer transactional data. According to co-founder Perret, he and Hockey came up  
 11 with the name “Plaid” based on the cross-hatch patterns formed when they mapped out how their  
 12 algorithm worked to compare consumers’ spending patterns with those of other consumers, while  
 13 also matching those consumers’ transaction data to Plaid’s nationwide merchant database.<sup>9</sup>

14 30. Not surprisingly, as fintech developers became aware of the scale and depth of  
 15 data Plaid could deliver, they also recognized its value to their own businesses.<sup>10</sup> One of the  
 16 earliest such developers was Venmo, whose head of development approached Plaid about  
 17 incorporating its software.<sup>11</sup> At that time, the main focus of Plaid’s software was the delivery of  
 18 extensive transaction data for the purpose of running analytics on the data.

19  
 20 <sup>6</sup> See <https://news.ycombinator.com/item?id=5216710>.

21 <sup>7</sup> See <https://news.ycombinator.com/item?id=5304169>. An Application Programming Interface is  
 22 a software intermediary that allows two applications to communicate with each other.

23 <sup>8</sup> See <https://news.ycombinator.com/item?id=5304169>.

24 <sup>9</sup> See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 10:45 to 11:45,  
<https://www.youtube.com/watch?v=sgnCs34mopw>.

25 <sup>10</sup> See *Plaid Launches the “Modern API for Banking Data,”*  
<https://homebrew.co/blog/2013/09/19/plaid-launches-the-modern-api-for-banking-data>  
 26 (“Everyone said ‘Yes, but where do we get that data? We’d absolutely love to use it.’ So Zach  
 and William decided to turn Plaid from an app into an API.”).

27 <sup>11</sup> See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 19:44 to 19:51,  
<https://www.youtube.com/watch?v=sgnCs34mopw>. At the time, Venmo was an independent  
 28 corporate entity registered in New York (Venmo LLC). In 2015, Venmo was acquired by PayPal,  
 Inc. and subsequently merged with that corporation.

31. During the following years, Plaid succeeded in getting its software embedded in a vast array of popular consumer-facing mobile and web-based fintech apps that enable ACH payments and transfers through consumers' financial accounts (collectively, "Participating Apps"), including popular apps such as Venmo, Coinbase, Square's "Cash App," and Stripe. Venmo had over 52 million active user accounts at the end of 2019;<sup>12</sup> Coinbase reportedly has more than 30 million users;<sup>13</sup> and Cash App reportedly has more than 24 million monthly active users.<sup>14</sup> Stripe's payment service reportedly is used by millions of businesses, and thus a commensurate number of consumers.<sup>15</sup> Plaid's own statistics indicate that Venmo and other payment apps make up over half of fintech app usage.<sup>16</sup>

**B. Plaid Deceptively Obtains Bank Account Credentials from App Users**

32. Plaid has achieved its success by accessing all of the data stored in consumers' financial accounts without consumers' knowledge or consent. The primary service offered by Plaid to the Participating Apps (*i.e.*, apps used by consumers to send and receive money from their financial accounts), is bank "linking" and verification. Verifying that a consumer owns a particular bank account is important for the safety and security of payment transfers using mobile apps. Fintech applications typically verify accounts either by making micro-deposits to a consumer's account, then requiring that the consumer report the amounts back to the app (which can take several days), or by asking a consumer to log in to their bank directly to confirm their identity as an account holder.

33. In a typical scenario, consumers log into their banks via an "OAuth" procedure, whereby users are redirected from the original webpage or app directly to their banks. There, consumers log into the bank's webpage or app, and then they are redirected back to the original

<sup>12</sup> See <https://investor.paypal-corp.com/static-files/0b7b0dda-a4ee-4763-9eee-76c01be0622c>.

<sup>13</sup> See <https://www.coinbase.com/about>.

<sup>14</sup> See <https://www.businessinsider.com/squares-cash-app-reached-24-million-users-and-monetization-surge-2020-2>.

<sup>15</sup> See <https://www.stripe.com/customers>.

<sup>16</sup> See Oct. 2016 Plaid Publication: *Financial data access methods: Creating a balanced approach*, Appendix C to Plaid's response to CFPB RFI, <https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf>.

1 app.<sup>17</sup> Behind the scenes, the bank returns a “token” that allows the original app to access the  
 2 consumer’s bank information as necessary and authorized by the consumer, but without giving  
 3 the app provider access to the login information.

4 34. Plaid has never adhered to the standard and secure OAuth procedure for the critical  
 5 process of having consumers log into their bank accounts. Instead, for the first several years of  
 6 Plaid’s operations, Plaid arranged for its fintech clients to collect consumers’ bank login  
 7 information and then pass that information to Plaid, which then approached the banks directly.<sup>18</sup>  
 8 In or around 2016, Plaid (belatedly, given the security risks) jettisoned this process for one even  
 9 more beneficial to Plaid.<sup>19</sup>

10 35. In or around 2016 Plaid implemented a method to *mimic* the OAuth procedure, but  
 11 Plaid’s method differs materially from a true OAuth process. Under this current system, Plaid  
 12 “directly collect[s]” credentials from the consumer. According to Hockey, the goal was not to  
 13 eliminate the security risk Plaid itself had created, but to “centralize[] that risk” at Plaid.<sup>20</sup>

14 36. Plaid refers to this new method as a “Managed OAuth” system. Plaid’s Managed  
 15 OAuth process has been incorporated in its “Plaid Link” software, which consists of software,  
 16 including login screens, developed by Plaid and distributed to its fintech clients for incorporation  
 17 into their apps.<sup>21</sup>

18 37. Plaid designs the login screens in its Managed OAuth interface to give them the  
 19 look and feel of login screens used by individual financial institutions (known as “spoofing”).  
 20 Because Plaid does not disclose it is not the actual bank, consumers are lulled into a false sense of  
 21 security by this login process, and this results in increased customer conversion. This process is  
 22 known as “phishing.”

23  
 24  
 25 <sup>17</sup> See, e.g., <https://www.oauth.com/oauth2-servers/redirect-uris/>.

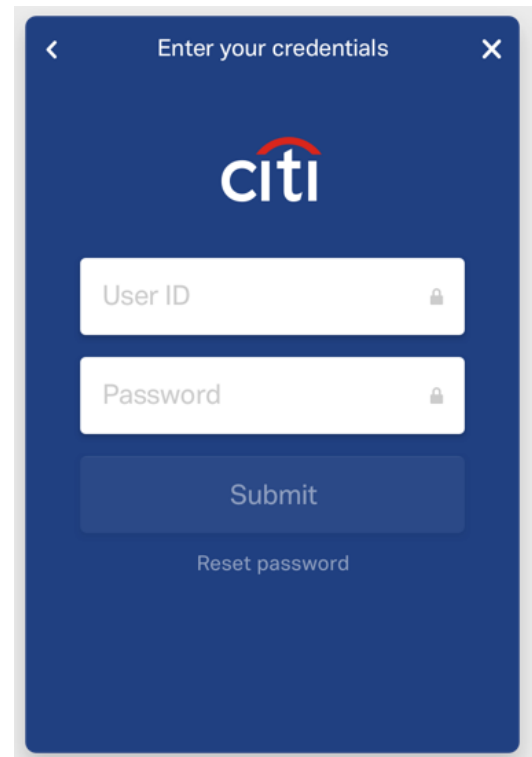
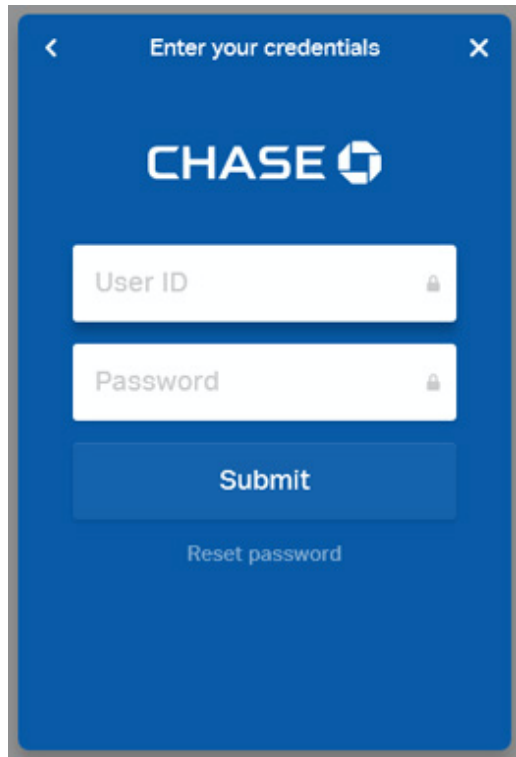
26 <sup>18</sup> See Sep. 26, 2018 Presentation by William Hockey, *Deep Dive w/ Plaid—William Hockey, Co-Founder & CTO*, at 13:54 to 14:09, <https://www.youtube.com/watch?v=9D5Rwt3DvGg>.

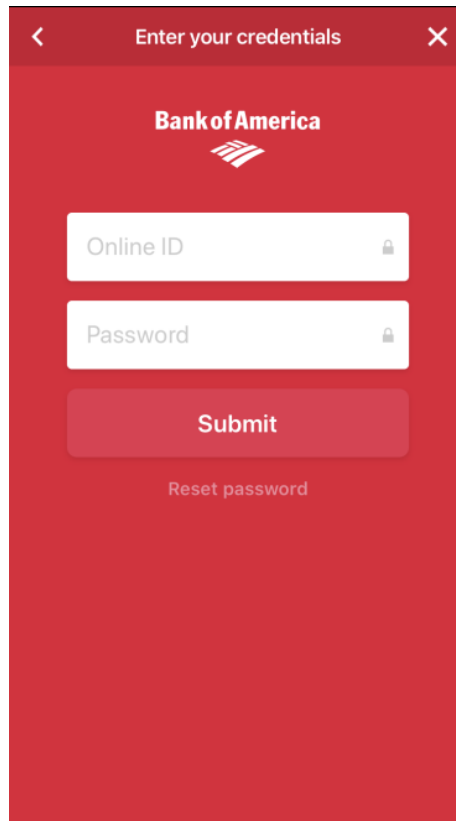
27 <sup>19</sup> *Id.* at 14:14 to 14:19.

28 <sup>20</sup> *Id.* at 14:39 to 14:55.

<sup>21</sup> See <https://fin.plaid.com/articles/demystifying-screenless-exchange/>.

38. For example, when consumers are prompted to verify their ownership of bank accounts for Venmo using a mobile device or web browser, they are asked to select their financial institution from an automatically generated list of bank logos, or to search for their institution if not shown. Immediately upon clicking on their chosen financial institution's logo, consumers are directed to a login screen branded with their chosen bank's logo and color scheme. From a consumer's perspective, the process appears to be the typical OAuth procedure that directs them to their bank to verify the account. Upon selecting a bank, the screen shifts and gives the impression that the user has been directed away from Venmo to interact with another entity, namely, their financial institution. In reality, they have been directed to a connection screen designed and inserted by Plaid *within* the Venmo app, and their communications are to Plaid instead of their trusted financial institution. The following are examples of Plaid's bank-branded login screens viewed in a mobile device:





39. Among other details appearing to confirm that the screen originates with the consumer's selected bank, Plaid's interface uses precise terms in the textboxes where users are told to enter their username and password that are consistent with the terms used by the banks themselves. Thus, for example, it says to enter the "User ID" for Chase Bank and Citi Bank, but the "Online ID" for Bank of America. The same pattern applies for other banks.<sup>22</sup> On these bank-branded Plaid login screens, consumers enter their login information. Instead of going straight to the bank, as would be the case in an OAuth procedure, the login information instead is transmitted directly to Plaid. Plaid then uses the information to access the consumer's bank account.

<sup>22</sup> Because Plaid's software is a template distributed for use by various fintech clients, the consumer experience across the Participating Apps is consistent in all material respects during any given time period. For the same reason, Plaid has the ability unilaterally to change the template viewable by consumers at any time without notice. The images above were captured in or around early 2020. As of the date of this filing, as at prior times in the class period, Plaid's use of bank logos and color schemes, and the overall design of the interface, remain deceptive.

40. Plaid’s use of bank logos and color schemes, and the overall design of the interface, are intentionally deceptive. In April 2016, Plaid’s Charley Ma stated in a comment thread on computer science and entrepreneurship site “Hacker News” that the company had “completely optimized” its “drop-in module used for onboarding bank accounts.”<sup>23</sup> A publication for developers on Plaid’s website from later that year sheds light on what this “optimization” entailed. In that publication, Plaid touted how “design elements” in its Managed OAuth process were key to the success of its software in “increasing user conversion,” including by customizing the “look and feel of permissioning access” for financial institutions.<sup>24</sup> In other words, Plaid specifically designed its system to have the appearance of a redirect-based OAuth system without actually redirecting the consumer to the bank’s website. And Plaid did so for the purpose of ensuring that the look and feel of its process would fool consumers into thinking they were actually logging into their bank rather than realizing that they were handing their login information to a third party.

41. In a 2017 blog post directed to its developer client audience, Plaid again conceded that Plaid’s login process was designed to mimic the look and feel of the bank’s website—including through the use of logos and bank-branded color schemes—“so that end-users feel a greater sense of security and familiarity.”<sup>25</sup>

42. Plaid’s scheme defies industry norms and consumers’ reasonable expectations. This is reflected, among other things, in the reaction of those few members of the app developer community who identified aspects of Plaid’s conduct. For example, in December 2018, Michael Kelly, a Plaid software engineer, was asked by a programmer in a now-deleted thread on Plaid’s GitHub page why Plaid fools users into thinking they are accessing their banks’ websites when logging in through Plaid:

<sup>23</sup> See Jun. 20, 2016 Y Combinator Hacker News thread: *Fintech Firm Plaid Raises \$44M*, <https://news.ycombinator.com/item?id=11939103>.

<sup>24</sup> See Nov. 15, 2016 Plaid Article: *Demystifying Screenless Exchange*, <https://fin.plaid.com/articles/demystifying-screenless-exchange/>.

<sup>25</sup> See Dec. 13, 2017 Plaid blog post: *Improving search for 9,600+ banks*, <https://blog.plaid.com/improved-search/>.

[Programmer]: givelively.org prompts me to provide my banking password on a web donation page. Browser inspector shows it's putting up a plaid.com iframe. That even renders my bank's logo to fool me into thinking I'm accessing my bank's site. This is absolutely unacceptable, regardless of what claims you make on your security page.

[Michael Kelly]: [W]e appreciate your concerns, which is why our compliance team vets anybody who uses Link. As to malicious knock offs, this is a matter that most successful companies lookout for and deal with -- as we and our security team do. If you see someone impersonating Link in such a way, please drop us a note at security@plaid.com. It's also worth noting that, in addition to the security we provide, banks protect their users from credential-based attacks via multi factor authentication.<sup>26</sup>

Kelly did not deny that Plaid was spoofing banks' websites, but instead only confirmed Plaid was aware that malicious parties could try to impersonate Plaid's method for phishing financial account credentials from fintech app customers.

43. Consumers themselves were left in the dark. For example, on a May 2018 Hacker News thread, Hockey responded to concerns about the collection of bank account transaction data via Plaid by pointing to whether a fintech app using Plaid (the app Robinhood) was *itself* collecting the data, thus deflecting awareness of Plaid's own misconduct:

[User]: "I would really caution connecting your bank account through Plaid on [Robinhood]. It's really unclear what data they are collecting but their privacy policy suggests they are collecting your bank account transaction history using Plaid's API. 100% a dealbreaker for me."

[Hockey]: "[C]o-founder of Plaid here. I can't give the rationale on why RH wrote the privacy policy the way they did, but I can guarantee you that they are not pulling transactional data. They're only using Plaid for the ACH authentication."<sup>27</sup>

Hockey failed to disclose the vital information that Plaid itself was collecting the banking data behind the scenes.

44. Plaid's conduct is particularly egregious in light of widespread financial industry recognition that it is improper to ask consumers to share their login information with third parties

<sup>26</sup> See Feb. 11, 2016 Github thread on Plaid "privacy/security concerns," <http://web.archive.org/web/20190415103059/https://github.com/plaid/link/issues/68>.

<sup>27</sup> See May 13, 2018 Y Combinator Hacker News thread: *Stock-trading app Robinhood was rejected by 75 investors*, <https://news.ycombinator.com/item?id=17060034>.



1 like Plaid. In October 2017, the Consumer Financial Protection Bureau (“CFPB”) released a set  
 2 of Consumer Protection Principles related to data aggregation services such as those offered by  
 3 Plaid. The CFPB recognized that one of the core principles for protecting consumers’ banking  
 4 data where it is being accessed by data aggregators is that such access should not “require  
 5 consumers to share their account credentials with third parties”—*i.e.*, credentials should not be  
 6 shared with parties other than the bank. Despite this official guidance, Plaid has persisted with its  
 7 practice of collecting consumer login information.

8 45. Whether under its original procedure or its even more sophisticated (and  
 9 deceptive) “Managed OAuth” procedure, Plaid has consistently structured the bank login process  
 10 in its software to allow it to intercept consumers’ bank login information. As the company  
 11 admitted in its February 2017 response to the CFPB’s Request for Information (“RFI”) regarding  
 12 consumer data access, “Plaid has developed a solution that passes credentials directly to the  
 13 trusted intermediary (Plaid).”<sup>28</sup>

14 46. In a December 2018 interview, Plaid’s Head of Engineering confirmed that the  
 15 following description of Plaid’s general method of capturing and using bank login information  
 16 was “90% accurate”: (1) set up a browser on a virtual machine, (2) have the user go to the bank’s  
 17 website, (3) have the user put in the banking credentials, and (4) scrape the screen to collect  
 18 banking data without the user knowing the difference.<sup>29</sup> Yet the difference is practically and  
 19 legally significant: Plaid never had consumers go to the bank’s website, but instead collected their  
 20 credentials directly.

21 47. Moreover, Plaid fails to properly protect the sensitive login credentials it acquires.  
 22 Plaid makes partial and deceptive representations to consumers that the software that accesses the  
 23 bank uses “end-to-end” encryption, thereby ensuring that the user’s login credentials “will never  
 24 be made accessible” to the Participating App. In reality, Plaid’s method of encryption is far from

25 <sup>28</sup> See Feb. 21, 2017 Response by Plaid to CFPB’s Consumer Data Access RFI,  
 26 <https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf>,  
 at 12.

27 <sup>29</sup> See Dec. 13, 2018 Software Engineering Daily Podcast: *Plaid: Banking API Platform with*  
 28 *Jean-Denis Greze*, <https://softwareengineeringdaily.com/2018/12/13/plaid-banking-api-platform-with-jean-denis-greze/>.



1 secure. Unlike banks and other financial institutions that include a second level of encryption as a  
 2 standard protection measure for customer login information handled through their apps, Plaid  
 3 uses a single level of encryption that leaves login credentials open to interception in plain text  
 4 form by a straightforward method that would be familiar to any malicious actor with even a  
 5 modicum of decryption expertise. That is, Plaid conceals both the fact of its obtaining banking  
 6 information, and the ramifications of having it afterwards.

7 **C. Plaid Leverages Credentials to Collect Valuable Data on a Massive Scale**

8 48. Plaid's deception has been successful, and inordinately profitable. By means of the  
 9 phishing bank login process embedded in the Participating Apps, and by using collected  
 10 consumer bank login information, Plaid has collected—and now stores, analyzes, and offers to its  
 11 fintech clients for sale—a staggering amount of consumer banking data.

12 49. Once Plaid captures a consumer's bank login credentials for the ostensible limited,  
 13 discrete purpose of verifying and linking a user's financial account to their chosen app, it actually  
 14 uses the credentials to obtain the maximum amount of data accessible to the consumer from the  
 15 bank. Plaid achieves this by approaching financial institutions under the pretense that Plaid's  
 16 access is permissioned by their consumer clients, and therefore the institution is legally required  
 17 by Section 1033 of the Dodd-Frank Act to provide Plaid with *all* available data concerning the  
 18 accounts in electronic form.<sup>30</sup>

19 50. From Plaid's earliest days, the company has collected what the co-founders have  
 20 described as an "immense" amount of consumer spending data and other information from banks.  
 21 With access to information going back up to five years, Plaid has taken detailed banking  
 22 information for thousands of transactions for each consumer—3,700 transactions on average—  
 23 that shows users' healthcare, educational, social, transportation, childcare, political, saving,  
 24 budgeting, dining, entertainment, and other habits, with an average of 1,750 unique geolocations  
 25 to which the transactions were mapped.<sup>31</sup>

26 <sup>30</sup> See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 16:34 to 17:19,  
 27 <https://www.youtube.com/watch?v=sgnCs34mopw>; see also 12 U.S.C. § 5533 (Dodd-Frank Act  
 28 Section 1033), which provides for consumer rights "upon request" to access financial account and  
 account-related data "in electronic form usable by consumers."

<sup>31</sup> See Feb. 2013 presentation by Zach Perret and William Hockey at NYC Data Business Meetup

1           51. As a result, even as early as February 2013, Plaid’s co-founders could tell industry  
2 insiders that the company was “generating one of the largest transactional data sets in the world.”<sup>32</sup>

3           52. Plaid generated this data set by engaging in still more unfair and unethical  
4 behavior. Plaid circumvented counter-measures employed by some banks to prevent data  
5 aggregators like Plaid from siphoning all information in a given consumer’s accounts by  
6 accessing accounts with the consumer’s credentials and “scraping” (*i.e.*, copying) data the banks  
7 would not share directly. Plaid’s insiders understood the unethical nature of the company’s  
8 method of gaining access to banks’ data stores. In August 2018, a former Plaid programmer  
9 responded to a Hacker News thread titled, *What is the most unethical thing you've done as a*  
10 *programmer?* The programmer identified his work for Plaid as one of the most unethical things  
11 he had ever done because, after consumers’ login credentials were obtained, Plaid developed  
12 methods for bypassing banks’ protections against data scraping<sup>33</sup> by using their status as an  
13 “affiliate” of banks’ downstream clients:

14                   [Plaid] needed to develop login integrations with consumer banks to  
15                   acquire customer account information for verification purposes. But  
16                   many such banks didn’t particularly want to grant them any special  
17                   API access. More importantly, these banks typically forbid scraping  
18                   and made it explicitly difficult by implementing JavaScript-based  
19                   computational measures required on the client in order to  
20                   successfully login. I helped [Plaid] develop methodologies for  
21                   bypassing the anti-scraping measures on several banking websites.  
22                   However, I stopped working on this because 1) I felt uncomfortable  
23                   with the cavalier way they were ignoring banks’ refusals, then using  
24                   the reversed integrations and onboarded customers as a bargaining  
25                   chip for more formal partnerships, and 2) performing huge amounts  
26                   of analytics on customer data acquired as part of the account  
27                   verification process.

28                   at 5:51 to 7:50, [https://www.youtube.com/watch?v=\\_I8DRbFmLKM](https://www.youtube.com/watch?v=_I8DRbFmLKM).

<sup>32</sup> See <https://news.ycombinator.com/item?id=5304169>.

<sup>33</sup> Data scraping is a technique in which a computer program extracts data from human-readable output coming from another program. Normally, data transfer between programs is accomplished using data structures suited for automated processing by computers, not people. The key element that distinguishes data scraping from automated computer data transfer is that the output being scraped is intended for display to an end-user, rather than as input to another program, and is therefore usually neither documented nor structured for convenient parsing. Data scraping is frequently done to interface with a third-party system that does not provide a more convenient API. In this case, the operator of the third-party system will often see screen scraping as unwanted due to, among other reasons, the loss of control of the information content. Consequently, data scraping is generally considered an *ad hoc*, inelegant technique used as a last resort when no other data interchange mechanism is available.

...

I don't have an issue with user data being mined for things like market research if it's a situation where the product is free and users can be easily made aware of it. But I find it dishonest if the company mining that data is doing so without direct user consent, or in a "backdoored" manner using their status as a downstream client's "affiliate" for T&C purposes.<sup>34</sup>

53. It bears emphasis that if a parent or guardian associates a bank account for their minor child with their own account, such that it is accessible with their own login credentials, even sensitive identifying information about the child would be swept into Plaid's data collection.

54. In May 2019, Perret confirmed that the scope of Plaid's data collection had grown to encompass tens of millions of consumers: "The scale has gotten immense. . . . *About one in four people in the US have linked an account with Plaid*, which means that we're kind of processing all the data coming through all those accounts on the other side."<sup>35</sup> The result, Perret explained, was that Plaid is storing what he described as "an immense pile of data," including the raw transactional data collected from banks and the data that Plaid is able to add by way of "enrichment" (e.g., location data that ties the transactions to a vast merchant database Plaid has compiled using that data).<sup>36</sup>

55. Plaid's Head of Engineering confirmed that the company stores the data it collects for backup purposes, that Plaid is "effectively caching" the banking data, and that it stores raw data in a permanent store.<sup>37</sup> As explained by Plaid in its Developer API documentation for app developers, Plaid automatically and consistently updates its cache of consumers' private financial and identifying information, every few *hours*, regardless of whether the consumer takes any further action:

<sup>34</sup> See Aug. 5, 2018 Y Combinator Hacker News thread: *What is the most unethical thing you've done as a programmer?*, <https://news.ycombinator.com/item?id=17692291>.

<sup>35</sup> See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 11:53 to 12:05, <https://www.youtube.com/watch?v=sgnCs34mopw>.

<sup>36</sup> *Id.* at 11:53 to 13:16.

<sup>37</sup> See Dec. 13, 2018 Software Engineering Daily Podcast: *Plaid: Banking API Platform with Jean-Denis Greze*, <https://softwareengineeringdaily.com/2018/12/13/plaid-banking-api-platform-with-jean-denis-greze/>.

We update a users [sic] account at set intervals throughout the day, independent of how many times a client calls the /connect endpoint. We pull transactions as they are posted to the issuing institution. Dependent on the merchant acquirer, processor, gateway and issuer, the time from when a transaction occurs to when it is posted can take from a couple minutes to a couple days.<sup>38</sup>

56. The information Plaid acquires also is not necessarily limited to data about the individual whose account was initially accessed for purported verification purposes. Once it has a consumer's login credentials, Plaid also pulls *any* transaction, address, contact, and other information in the accounts—whatever is available. Plaid thus also obtains information about any joint account holders, authorized users, and even about related accounts used for a consumer's minor children.

57. In the January 13, 2020 press release and accompanying presentation announcing Visa's purchase of Plaid, Visa reiterated that Plaid has the banking information of one in four people with a U.S. bank account, including the banking data from over 200 million accounts.<sup>39</sup> Venmo users alone accounted for a large portion of those consumers and accounts, given that Venmo had over 52 million users as of the end of 2019.<sup>40</sup>

58. According to the Visa/Plaid press release, Plaid is used by thousands of digital financial apps and services, and accesses data at over 11,000 financial institutions across the U.S., Canada and Europe.<sup>41</sup> Indeed, the scale of Plaid's data aggregation is reflected in the magnitude of Visa's purchase price: according to the deal, Visa would pay \$4.9 billion in cash and approximately \$400 million in retention equity and deferred equity.<sup>42</sup>

<sup>38</sup> See <https://plaid.com/docs/legacy/api/>.

<sup>39</sup> See Jan. 13, 2020 Press Release: *Visa To Acquire Plaid*, <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.16856.html>; see also accompanying presentation, [https://s1.q4cdn.com/050606653/files/doc\\_presentations/2020/Visa-Inc.-To-Acquire-Plaid-Presentation.pdf](https://s1.q4cdn.com/050606653/files/doc_presentations/2020/Visa-Inc.-To-Acquire-Plaid-Presentation.pdf).

<sup>40</sup> See <https://investor.paypal-corp.com/static-files/0b7b0dda-a4ee-4763-9eee-76c01be0622c>.

<sup>41</sup> See <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.16856.html>; <https://fortune.com/2020/01/14/visa-plaid-acquisition-fintech/>.

<sup>42</sup> See [https://s1.q4cdn.com/050606653/files/doc\\_presentations/2020/Visa-Inc.-To-Acquire-Plaid-Presentation.pdf](https://s1.q4cdn.com/050606653/files/doc_presentations/2020/Visa-Inc.-To-Acquire-Plaid-Presentation.pdf).

**D. Plaid Sells and Otherwise Exploits the Unlawfully-Obtained Private Data**

59. Plaid has admitted that it routinely sells the consumer banking data it collects. At a minimum, Plaid sells the data it obtains from consumers' accounts back to the very app providers, including the Participating Apps, who use its services.<sup>43</sup> Plaid calibrates its prices based on the type of information being sold.<sup>44</sup>

60. Plaid fails to exercise control or oversight into how these companies store and use the sensitive banking and other private consumer data they purchase from Plaid, or what those companies do with the data after purchasing it. Instead, Plaid purports to rely upon an initial vetting process and a boilerplate Developer Policy with vague terms like "best practices" and "applicable laws": "Your systems and application(s) must handle End User Data securely. With respect to End User Data, you should follow industry best practices . . . . Any End User Data in your possession must be stored securely and in accordance with applicable laws."<sup>45</sup>

61. Plaid's vetting process is inadequate to ensure that the thousands of applications paying Plaid for access to the sensitive consumer data it delivers are complying with legal requirements like those imposed by the Gramm-Leach-Bliley Act ("GLBA"), California's Financial Information Privacy Act ("CalFIPA"), and California's Online Privacy Protection Act ("CalOPPA"). Plaid has no ability to track what companies like the Participating Apps do with the consumer data they purchase from Plaid.

62. Plaid also has arranged to sell the vast store of private financial data it possesses to Visa via Visa's purchase of the company for \$5.3 billion.

63. In addition to selling raw data, Plaid derives additional valuable benefits for its business by analyzing the private information it obtains from consumers, including by "using machine learning to draw insights about how consumers spend their time, money, and

<sup>43</sup> See Feb. 21, 2017 Response by Plaid to CFPB's RFI, <https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf> (Plaid acknowledges to CFPB that it sells data to party "permissioned" by consumer).

<sup>44</sup> See Feb. 2019 interview with Zach Perret, <https://www.saastr.com/build-a-platform-ecosystem/>.

<sup>45</sup> See <https://plaid.com/legal/>.

1 attention.”<sup>46</sup> In August 2018, a programmer who formerly worked for Plaid confirmed that the  
 2 company “perform[ed] huge amounts of analytics on customer data acquired as part of the  
 3 account verification process.” The programmer also highlighted the economic value of the  
 4 analytics Plaid performs on the banking data, explaining how the data may be monetized by  
 5 selling the “derivative analytics” of the data to hedge funds, who use the analytics to forecast the  
 6 revenue of companies in advance of equity earnings announcements.<sup>47</sup>

7 64. As Perret explained in May 2019, Plaid’s long-term business plan is to monetize  
 8 the mountain of private banking data it has collected. The company is in “phase one,” scaling up  
 9 its business and gathering and enriching as much information about consumers’ financial and  
 10 private lives as possible, but ultimately Plaid plans to make a large-scale pivot toward monetizing  
 11 that data through analytics and the provision of what it calls “value-added services.” As a result,  
 12 the company employs a large data science team that works on applying sophisticated analytics to  
 13 the data Plaid has illicitly obtained, with the end goal of developing products for other fintech  
 14 applications based upon the data and analytics. As Perret put it, over time Plaid’s focus will  
 15 become “more and more about analytics” (*i.e.*, generating data-based profiles of consumers and  
 16 their habits) and providing “value-added services on top of the data that’s coming through the  
 17 system.”<sup>48</sup>

18 65. The data Plaid has accumulated from consumers through material omissions and a  
 19 series of unfair and unethical actions that invade their privacy has provided the company with a  
 20 serious competitive advantage. In 2018, Plaid investor Goldman Sachs cited the “sustainable  
 21 moat or advantage” provided by Plaid’s data network effects, where developers are forced to rely  
 22 upon Plaid’s technology even to understand their own users’ behavior.<sup>49</sup>

23 <sup>46</sup> See Jul. 1, 2015 Y Combinator Hacker News thread,  
 24 <https://news.ycombinator.com/item?id=9812245>.

25 <sup>47</sup> See Aug. 5, 2018 Y Combinator Hacker News thread: *What is the most unethical thing you've*  
*done as a programmer?*, <https://news.ycombinator.com/item?id=17692291>.

26 <sup>48</sup> See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 14:21 to 14:26,  
 27 <https://www.youtube.com/watch?v=sgnCs34mopw>.

28 <sup>49</sup> See Oct. 4, 2018 CNBC article: *Meet the start-up you’ve never heard of that powers Venmo,*  
*Robinhood and other big consumer apps*, [https://www.cnbc.com/2018/10/04/meet-the-startup-](https://www.cnbc.com/2018/10/04/meet-the-startup-that-powers-venmo-robinhood-and-other-big-apps.html)  
[that-powers-venmo-robinhood-and-other-big-apps.html](https://www.cnbc.com/2018/10/04/meet-the-startup-that-powers-venmo-robinhood-and-other-big-apps.html).

1           **E.     Plaid and Its Fintech Clients Conceal Plaid’s Conduct from Consumers**

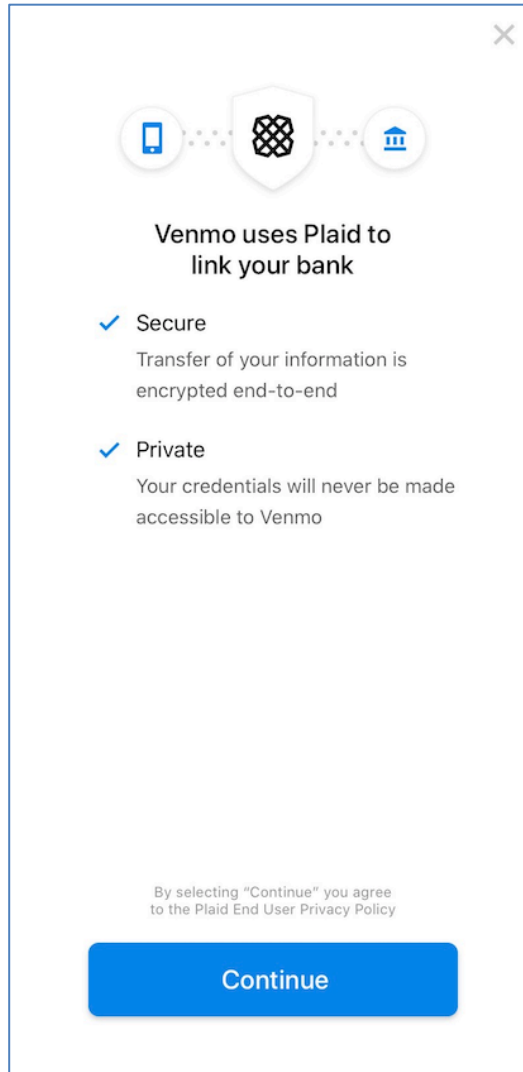
2           66.     Plaid distributes to each of its fintech clients a template for use in guiding  
3 consumers through the process of linking their financial accounts to the app. Some apps, such as  
4 Square’s Cash App, do not even make use of the template and provide no disclosures whatsoever,  
5 simply directing consumers to select a bank and input their credentials. In all events, at no time  
6 are users of any of the Participating Apps informed that Plaid will receive and retain access to  
7 their financial institution account login credentials. Nor are they informed that Plaid or any party  
8 would use those credentials to collect information from their financial accounts on the scale and  
9 for the duration that actually occurs, let alone that data *not* collected by the fintech clients in the  
10 first instance would be made available to them for purchase. Plaid is responsible for ensuring  
11 proper disclosures to consumers, both in the content of its own privacy policy and disclosures,  
12 and in the privacy-related disclosures in the Plaid software incorporated in the apps of companies  
13 through which Plaid interacts with consumers. Plaid has failed to ensure that appropriate  
14 disclosures were actually made to consumers using those apps.

15                   **1.     Venmo: An Illustrative Example**

16           67.     As an illustrative example, when Venmo users are prompted to connect to their  
17 bank account in the app, they are directed to the first screen in the Plaid Link software flow,  
18 which appeared as follows as of early 2020<sup>50</sup>:

19  
20  
21  
22  
23  
24  
25  
26  
27  
28           <sup>50</sup> As described below, Plaid made certain changes to this screen in its Plaid Link software later in 2020, shortly after the initial complaint was filed in this consolidated action, and apparently in response to this lawsuit.





68. The largest text at the top of the screen stated, “Venmo uses Plaid to link your bank.” Smaller text underneath stated, “Secure: Transfer of your information is encrypted end-to-end,” and underneath that was the assurance: “Private: Your credentials will never be made accessible to Venmo.”

69. At the bottom of that screen was a large, bright blue “Continue” button. Just above that button there was text in a still smaller, lighter grey font, stating, “By selecting ‘Continue’ you agree to the Plaid End User Privacy Policy.” There was no visual indication that the latter text was a clickable hyperlink. In fact, however, if the user clicked on that text, they were redirected to Plaid’s privacy policy on its website, located at <http://plaid.com/legal/#end-user-privacy-policy>. The hyperlink was deemphasized in multiple ways, including by failing to underline it (which may signal the presence of a hyperlink), by using a font size that is smaller than text used



1 elsewhere on the screen, and by using a lighter grey color for the text than used elsewhere on the  
 2 screen, with the lighter grey text set against a light background. As a result, it was not knowable  
 3 to a reasonable user that the text was a hyperlink unless and until the small text was actually  
 4 pressed. There were no other elements on the screen directing the user to the existence of the  
 5 hyperlink. Similarly, there was nothing on this or any subsequent screen that required the user to  
 6 actually read through the linked policy, indicate that the terms have been read, or indicate  
 7 acceptance of the terms of the policy.<sup>51</sup>

8         70. This screen in the Venmo app (which is the same in form, color, and substance for  
 9 each Participating App except that the name of the app can be customized, as well as whether the  
 10 blue button says “Continue,” “Ok,” “Get Started,” or “Agree”) contained no description of what  
 11 Plaid is or what it does, such as a disclosure that Plaid is a completely separate company  
 12 operating independently of Venmo that intends to establish a long-term connection to the  
 13 consumer’s bank account and siphon all available private information. There was no indication  
 14 whatsoever in the app or throughout the process that a Venmo user had gone from interfacing  
 15 with Venmo to interfacing with any third party other than their own bank.

16         71. In the unlikely event the user saw the fine-print text, decided to test whether it was  
 17 a hyperlink, and then actually clicked on the link, they were redirected to the beginning of Plaid’s  
 18 lengthy privacy policy webpage. If the user then took the time to scroll and read through the  
 19 policy (although nothing to this point alerted the user to the possibility that their private data may  
 20 even be at stake), they would eventually find only this statement:

21                 Information we collect from your financial accounts. The  
 22                 information we receive from the financial product and service  
 23                 providers that maintain your financial accounts varies depending on  
 24                 the specific Plaid services developers use to power their  
 25                 applications, as well as the information made available by those  
 26                 providers. But, in general, we collect the following types of  
 27                 identifiers, commercial information, and other personal information  
 28                 from your financial product and service providers:

---

27 <sup>51</sup> Plaid’s privacy policy is no better disclosed to users of other Participating Apps. The screens  
 28 presented to users of Coinbase, for example, present users with a screen identical in all material  
 respects as Venmo. Square’s Cash App presents no screen containing reference to “Plaid” or its  
 privacy policy at all, and simply directs users to a page to “[s]elect [their] bank.”

- Account information, including financial institution name, account name, account type, account ownership, branch number, IBAN, BIC, and account and routing number;
- Information about an account balance, including current and available balance;
- Information about credit accounts, including due dates, balances owed, payment amounts and dates, transaction history, credit limit, repayment status, and interest rate;
- Information about loan accounts, including due dates, repayment status, balances, payment amounts and dates, interest rate, guarantor, loan type, payment plan, and terms;
- Information about investment accounts, including transaction information, type of asset, identifying details about the asset, quantity, price, fees, and cost basis;
- Identifiers and information about the account owner(s), including name, email address, phone number, date of birth, and address information;
- Information about account transactions, including amount, date, payee, type, quantity, price, location, involved securities, and a description of the transaction; and
- Professional information, including information about your employer, in limited cases where you've connected your payroll accounts.

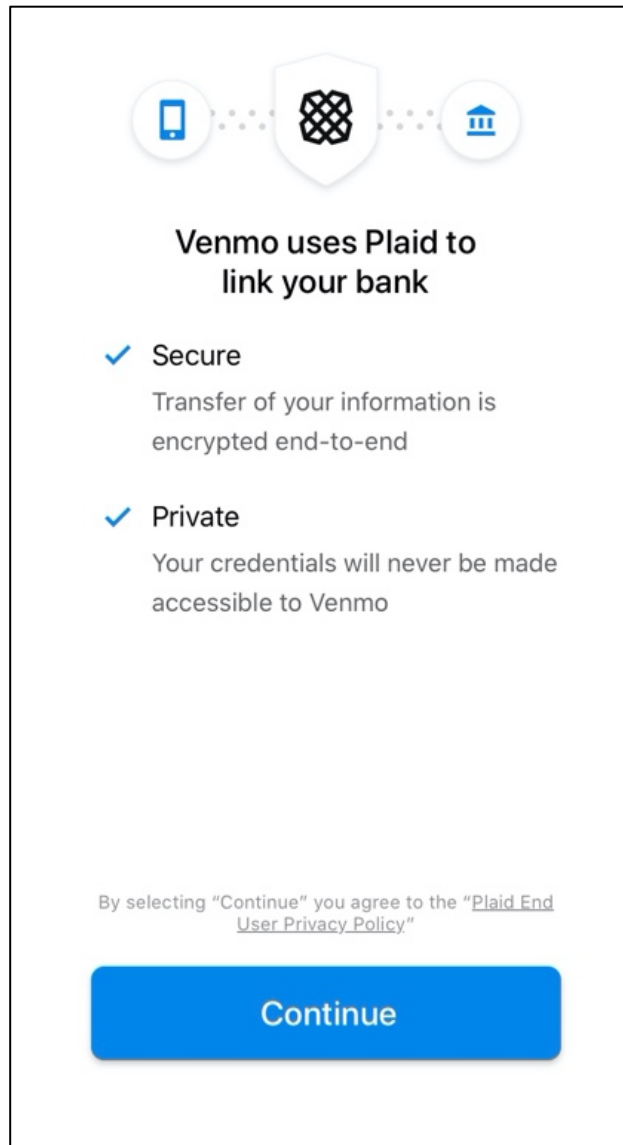
The data collected from your financial accounts includes information from all your accounts (e.g., checking, savings, and credit card) accessible through a single set of account credentials.<sup>52</sup>

## **2. Recent Changes to Venmo's Software**

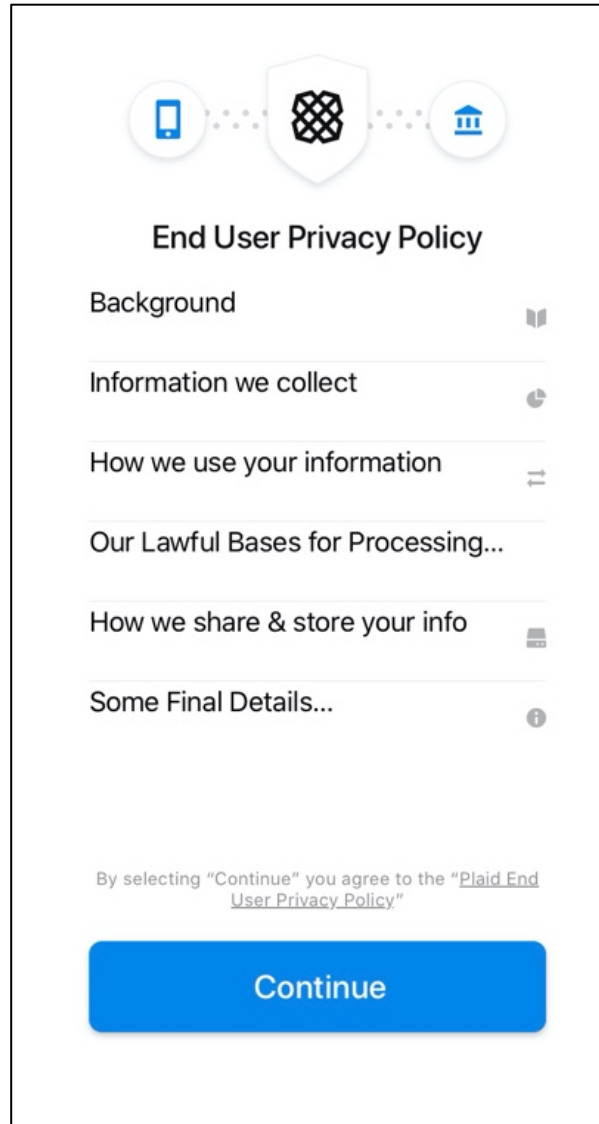
72. As noted above, shortly after this action was filed, Plaid redesigned certain aspects of the Plaid Link software incorporated in Venmo. The latest version of Plaid's software incorporated in Venmo now appears as follows:

---

<sup>52</sup> See Plaid Privacy Policy, <https://plaid.com/legal/#end-user-privacy-policy> (emphasis added). See *infra*, Section V.G.3, for further discussion of these terms.



Thus, the text linking to Plaid's privacy policy has been changed by putting "Plaid End User Privacy Policy" in quotes and underlining the text. Unlike the prior version, the text no longer contains a hyperlink to Plaid's privacy policy on Plaid's website. Instead, the text acts as a button in the Venmo app, opening a new screen in the Plaid Link software:



This screen contains no indication of how consumers should navigate to see the actual terms of Plaid’s privacy policy. For example, the same language that appeared on the prior screen still appears above the “Continue” button, but pressing the underlined language does nothing. Only if the consumer independently decides to press on one of the headings or to scroll down on the screen do the terms of the privacy policy become visible.

73. None of the recent changes Plaid made to its Plaid Link software following the filing of this lawsuit have cured the deceptive nature of that software.

### 3. The Deceptive Nature of Plaid's Software

74. Plaid's software incorporated in the Venmo app is illustrative of the way Plaid conceals the true facts from consumers:

a. The manner in which Plaid's software is incorporated into the Venmo app is not fully disclosed, and, more importantly, nowhere is it disclosed that Plaid uses bank login information to access consumers' accounts.

b. Multiple statements in the Plaid software incorporated in the Venmo app have a tendency to deceive consumers. Users are told they need to "sign in" to their bank accounts. They receive promises that the system is "Private," and that the consumer's "credentials will never be made accessible to Venmo." In fact, the system is designed not to be private because it requires passing credentials to Plaid as a third-party data aggregator and also includes the wholesale looting of the consumer's most private banking data. By stating that the login credentials will not be made accessible to Venmo, consumers are falsely led to reasonably expect that their credentials are not shared at all during the account verification process, other than with the bank they know and trust, while in fact those credentials are intercepted by Plaid for its use in gathering data from the bank. In addition, Plaid's failure to implement a second level of encryption, consistent with the practice of legitimate financial institutions, leaves consumer credentials vulnerable to interception in plain text form by malicious actors with even minimal decryption expertise.

c. Another statement in the Plaid software incorporated in the Venmo app that is deceptive on its own and relevant for what it does *not* disclose is the promise that the system is "Secure," and that the consumer's information is "encrypted end-to-end." In fact, the system is designed not to be secure, including because: (i) Plaid uses it to collect, sell, use, and store consumers' most private financial data; (ii) Plaid fails to exercise control or oversight over how that data is stored or used after it sells it to Venmo; and (iii) when Plaid removes consumer banking data from the secure banking environment, it thereby destroys valuable protections afforded to consumers in the event of data breach or theft. And by stating that the consumer's information is encrypted end-to-end, consumers are falsely led to believe that no entity outside of

1 Venmo and the bank ever receives access to any consumer information. In addition, Plaid's  
2 failure to implement an industry-standard second level of encryption renders its system unsecure  
3 by leaving consumer credentials vulnerable to interception in plain text form by malicious actors  
4 with even minimal decryption expertise.

5 d. Plaid's practice of spoofing bank login websites in its software—including  
6 without limitation by the design, context, and performance of the application—deceives  
7 consumers as to the existence of Plaid as a separate entity, Plaid's status as a third party, the fact  
8 that Plaid collects consumer bank login information directly, and the fact that Plaid uses bank  
9 login information to access consumers' accounts. It instead is intended to deceive consumers into  
10 believing that they are entering their bank login directly at the bank's website, as would be the  
11 case in a standard, redirect-based OAuth procedure.

12 e. The link in the Venmo app to Plaid's privacy policy is deemphasized and hidden  
13 from the consumer's attention, including through its placement; the size and color of the font  
14 used; the lack of underlining or other means of notifying the consumer that the text is actually a  
15 hyperlink; the reasonable expectation a consumer would have about the level of disclosure that  
16 would be provided in advance of divulging sensitive financial data to a third party; and, by  
17 contrast, the diminutive nature of the text used for the hyperlink as compared to other text and  
18 other surrounding elements incorporated on the screen.

19 f. The Plaid software incorporated in the Venmo app fails to require affirmative  
20 consumer permission for Plaid to access, sell, use or store any consumer banking information.

21 g. The Plaid software incorporated in the Venmo app uses a "fine-print click-  
22 through" disclosure process that is inadequate to establish knowledge or consent to Plaid's  
23 practices by consumers, even if the policy itself had fully and sufficiently disclosed Plaid's true  
24 conduct (which it did not).

25 h. Plaid's privacy policy fails to disclose the following facts: (i) Plaid collects  
26 consumer bank login information directly; (ii) Plaid uses bank login information to access  
27 consumers' accounts; (iii) Plaid collects all available private financial and other identifying data  
28 from every available account once it accesses the "linked" account; (iv) Plaid sells the consumer

1 banking data it collects to its clients; (v) Plaid does not exercise adequate oversight over how  
 2 consumer banking data is stored or used after it sells that data to Venmo; (vi) Plaid otherwise  
 3 uses and monetizes the consumer banking data it collects; (vii) Plaid stores the consumer  
 4 banking data it collects; (viii) Venmo purchases, uses, and stores the consumer banking data  
 5 collected by Plaid; (ix) Plaid continues to access accounts and collect, sell and use consumer  
 6 banking data after the initial connection is made, regardless of whether the consumer continues  
 7 using the Venmo app; and (x) by removing consumer banking data from the secure banking  
 8 environment, Plaid is destroying valuable protections afforded to consumers in the event of data  
 9 breach or theft.

10 i. Plaid falsely implies limitations to its data aggregation practices in its privacy  
 11 policy in stating that the information it gathers from financial institutions “varies depending on  
 12 the specific Plaid services developers use to power their applications.” In fact, Plaid collects all  
 13 available consumer banking information when it connects with a consumer’s account, whether or  
 14 not Venmo ultimately requests its own access to the data, and regardless of whether the data has  
 15 any relevance to transactions on Venmo. The most basic Plaid “tier” for app developers always  
 16 includes Plaid’s “Transactions” product (*i.e.*, the option to access years of historical account  
 17 activity), for example, because Plaid collects all transaction information as a matter of course.<sup>53</sup>

18 j. By Plaid stating in its privacy policy that the company collects “[i]nformation  
 19 about account transactions, including amount, date, payee, type, quantity, price, location,  
 20 involved securities, and a description of the transaction,” Plaid deceives consumers who use  
 21 Venmo into believing that it only collects information about transactions conducted using the  
 22 Venmo app. Plaid thereby conceals the fact that it collects years’ worth of transaction  
 23 information entirely unrelated to the consumer’s use of Venmo.

24 75. Plaid designs and employs its software to ensure that none of the Participating  
 25 Apps disclose Plaid’s conduct described herein to consumers.

26 76. As a result of Plaid’s inadequate and misleading disclosures, consumers have been  
 27 kept in the dark about the role Plaid plays in the relationship between consumers, fintech apps,

28 <sup>53</sup> See <https://plaid.com/pricing/>.

1 and financial institutions. Indeed, it was Plaid’s plan from the beginning, as Hockey explained,  
 2 that “most people will never know we exist.”<sup>54</sup> And in a 2019 interview, Perret confirmed that  
 3 Plaid believes consumers “never need to know” they are using Plaid, and Plaid doesn’t “need  
 4 every consumer to know who Plaid is”; to the contrary, the only thing Plaid wants consumers to  
 5 know is that they are using a fintech app.<sup>55</sup> The vast majority of consumers therefore have no idea  
 6 that Plaid even exists, much less that it has collected, stored, sold, and is using their most  
 7 sensitive and private financial information.

8 77. In an October 2018 article on Plaid, CNBC reported that “[d]espite popularity with  
 9 coders, the average person interacting with Plaid most likely wouldn’t recognize the company”  
 10 and the fact that it “quietly powers” Venmo and many other apps. The article also reveals that  
 11 Plaid’s largest investors were well aware that consumers have no idea about Plaid or its role with  
 12 those apps: “‘Plaid has quietly created a very big infrastructure *without the consumer knowing*  
 13 *that they’re powering it,*’ said Christopher Dawe, co-head of private investment at Goldman  
 14 Sachs Investment Partners . . . , who led Goldman’s 2016 Series B investment in Plaid . . . .”<sup>56</sup>

15 **F. Plaid’s Harm to Consumers is Recognized by Banks and Industry Groups**

16 78. Because of Plaid’s deficient disclosures and active concealment of the true state of  
 17 affairs, consumers using the Participating Apps are unaware that their financial data has been  
 18 extracted, analyzed, and sold by Plaid. Banks and other sophisticated industry groups, however,  
 19 have been rightfully concerned about the actions of data aggregators like Plaid for some time. In  
 20 JPMorgan Chase’s April 2016 shareholder letter, for example, the CEO stated that the bank had  
 21 analyzed many third-party contracts providing consumer banking data access to outside entities  
 22 such as payment providers and data aggregators. The bank concluded that: (1) “[f]ar more  
 23 information is taken than the third party needs in order to do its job”; (2) “[m]any third parties sell

24 <sup>54</sup> See Aug. 2013 emorywire article: *To Hack and Disrupt*,  
 25 [http://www.alumni.emory.edu/emorywire/issues/2013/august/of\\_interest/story\\_1/index.html#.Xk sqMxNKjQg](http://www.alumni.emory.edu/emorywire/issues/2013/august/of_interest/story_1/index.html#.Xk sqMxNKjQg).

26 <sup>55</sup> See Feb. 2019 interview with Zach Perret at 19:08 to 19:37, <https://www.saastr.com/build-a-platform-ecosystem/>.

27 <sup>56</sup> See Oct. 4, 2018 CNBC article: *Meet the start-up you’ve never heard of that powers Venmo,*  
 28 *Robinhood and other big consumer apps*, <https://www.cnbc.com/2018/10/04/meet-the-startup-that-powers-venmo-robinhood-and-other-big-apps.html> (emphasis added).



1 or trade information in a way customers may not understand, and the third parties, quite often, are  
 2 doing it for their own economic benefit – not for the customer’s benefit”; and (3) “this is being  
 3 done on a daily basis for years after the customer signed up for the services, which they may no  
 4 longer be using.” He also stated: “When customers give out their bank passcode, they may not  
 5 realize that if a rogue employee at an aggregator uses this passcode to steal money from the  
 6 customer’s account, the customer, not the bank, is responsible for any loss. . . . This lack of clarity  
 7 and transparency isn’t fair or right.”<sup>57</sup>

8 79. In February 2017, the American Bankers Association provided a response to the  
 9 CFPB’s RFI, identifying numerous concerns and issues with the practices of data aggregators  
 10 such as Plaid, including the following:

11 (a) Unknowing Grant of Unlimited Access

12 “Current practices in the data aggregation market . . . may leave  
 13 consumers exposed and create risk that undermine this trust.  
 14 Consumers today are offered a Faustian bargain in which their  
 15 desire for technology-driven convenience is exchanged—often  
 16 unknowingly—for increased potential of catastrophe, by handing  
 17 over the keys to their financial vault. When consumers share their  
 18 login credentials with an aggregator, they are giving the aggregator  
 19 *carte blanche* access to their financial data, including information  
 20 about things such as their life savings or retirement account. Yet  
 21 consumers are not given adequate information or control over what  
 22 information is being taken, how long it is accessible, and how it  
 23 will be used in the future.”<sup>58</sup>

24 (b) Unknowing Removal of Sensitive Information from Secure  
 25 Environment

26 “Moreover, consumers are unaware of the differences in the legal  
 27 and supervisory standards applicable to bank and nonbank  
 28 participants in the financial services marketplace. Once the  
 information is shared, it leaves a secure bank environment, where it  
 is accorded longstanding legal protections, and it is released into the  
 data services market where it is accorded no more special status  
 than data created through a consumer’s use of a social media  
 platform.

57 See Apr. 6, 2016 Letter from JPMorgan Chase to shareholders,  
<https://www.jpmorganchase.com/corporate/annual-report/2015/>.

58 See Feb. 21, 2017 Response by American Bankers Association to CFPB RFI,  
<https://buckleyfirm.com/sites/default/files/Buckley%20Sandler%20InfoBytes%20-%20American%20Bankers%20Association%202017.02.21%20Comment%20Letter%20to%20CCFPB%27s%20RFI%20CFPB-2016-0048.pdf>.

...

When consumers allow data aggregators to access their data they run the risk – often unknowingly – associated with moving their data out of the secure banking environment, where it is fully protected by law, and moving it into the data services market where it is not accorded appropriate protections. More troubling is that a number of these non-bank consumer financial data service providers take the position that financial data are no different from any other form of data, and as such ignore or avoid any protections that should be afforded it. Furthermore, the lack of transparency and control, and the liability limits asserted by the aggregator, all work to the consumer’s disadvantage.”<sup>59</sup>

(c) Access Unlimited as to Scope or Time

“Today, when consumers provide their access credentials to a data aggregator, they are giving that company access to any information that is housed in their online bank account, and they give access for an unlimited period of time. There is little effort to inform consumers about the information being taken, how it is being used or shared, how often it is being accessed, and how long the aggregator will continue to access it.”<sup>60</sup>

(d) Access to Unnecessary Data

“Consumers assume that data aggregators take only the data needed to provide the service requested. However, too often it is not the case.”<sup>61</sup>

(e) Use and Sale of Banking Data

“Many data aggregators use the data for purposes beyond the specific service that the customer sought. Access to all data enables the aggregator to profit by selling the information to other third parties even though the customer neither knew about that potential use nor requested any additional services or marketing.”<sup>62</sup>

(f) Increased Risk of Identity Theft

“The risks to consumers should not be minimized. First, the sheer volume and value of the aggregated data make data aggregators a priority target for criminals, including identity thieves. This is because data aggregators collect and share information from multiple

---

<sup>59</sup> *Id.*

<sup>60</sup> *Id.*

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*

financial institutions which is a vast expansion of the information held at any one bank. Thus, data aggregators may have the financial information, including account credentials, for the accounts across a consumer's entire financial portfolio. Through a single source, the criminal may gain access to the consumer's checking and savings accounts, retirement accounts, certificates of deposits, credit cards, brokerage accounts, and insurance products. Also, increasingly data aggregators have the ability to conduct transactions, such as sending remittances, on behalf of consumers. This rich reward for a single hack, either of an aggregated database of personally identifiable information or of a single consumer's multiple accounts, makes data aggregators an attractive target for criminals. They obtain the key not to just a single room, but the key ring with keys to all the rooms.

[T]he impact on the consumer in the event of a compromise can be far greater than a single-financial institution compromise. With the consumers' credentials and account information, criminals may drain deposit accounts, liquidate stocks, and max out credit cards. Even if consumers are ultimately reimbursed, they may suffer crippling inconvenience from even a temporary loss of access because the unauthorized access involves all their financial accounts. They may have no access to funds for day-to-day living. Important payments may be returned unpaid, stocks may be sold at disadvantageous prices, and schedules and peace of mind will be upended as they attempt to recover their assets."<sup>63</sup>

80. Some banks have rightly rejected Plaid's assertions that consumers authorize its conduct, and have taken extreme measures to protect their customers from Plaid. In December 2019, the Wall Street Journal reported on PNC Bank's actions in upgrading its security systems to prevent Plaid from accessing its banking customers' information for Venmo and other apps. PNC's head of retail banking, Karen Larrimer, was quoted in the article as justifying the bank's actions based upon Plaid's storage of account access information "indefinitely, often unbeknownst to customers," putting customers and their money at risk.<sup>64</sup>

81. Larrimer further explained in a subsequent article that PNC's position is that many consumers do not fully understand what happens to their data when they sign up for an app, and an aggregator such as Plaid is involved behind the scenes. One thing many consumers do not

---

<sup>63</sup> *Id.*

<sup>64</sup> See Dec. 14, 2019 Article: *Venmo Glitch Opens Window on War Between Banks, Fintech Firms*, <https://www.wsj.com/articles/venmo-glitch-opens-window-on-war-between-banks-fintech-firms-11576319402>.

recognize, Larrimer explained, is that once access has been obtained to one banking account, the aggregator “can scrape every piece of information that is in your banking relationships—any other accounts you have, any loans you have, any transaction data, whatever is there they have full access to.” Larrimer also explained that the bank was concerned about lack of consumer knowledge of where their data is being stored, for how long it is stored, or for what purposes it is being used.<sup>65</sup>

82. These concerns raised by banks and industry groups are valid. Plaid collects, sells, and uses the most sensitive consumer banking data on a shockingly large scale by employing its Managed OAuth procedure and hiding its activity from consumers.

**G. Plaid Knowingly Violates Established Industry Standards and Obligations**

83. Plaid’s omissions, non-disclosures, misdirection, and active concealment represented in Plaid’s statements described herein; throughout the template-based account verification and linking process; throughout Plaid’s process for obtaining information about consumers from their financial accounts; and in Plaid’s use, analysis, and sale of that information and insights derived from it, all violate consumers’ reasonable expectations and industry norms.

84. Established industry standards prohibit intrusions such as Plaid’s into consumers’ private information. For example, in testimony before the House Financial Services Committee Task Force on Financial Technology, on November 21, 2019, a representative for the American Banker’s Association explained that the association had “developed a set of principles – consistent with the CFPB and the rest of industry,” to help protect consumers in the context of financial data aggregation. Those principles include:

**Transparency** – Consumers must have transparency about how companies use their financial data. It should be clear to consumers what data a technology company are accessing, how long the company is holding this data, and how it is using the data.

**Control** – When consumers share their financial data they should have control over what information is shared and how it is used. Intuitive control would allow consumers to see easily who is

<sup>65</sup> See Jan. 2020 Article: *PNC Bank Counters ‘P2P War’ Speculation Over Its Venmo App Moves*, <https://thefinancialbrand.com/91550/pnc-bank-p2p-venmo-mobile-app-zelle-plaid-aggregator/>.

authorized to receive their data, modify what access they have, and revoke that access when a service is no longer used.

**Minimization** – Consumers should expect that data-sharing is limited to the data that are needed to provide the service they have authorized and only maintain these data as long as necessary.<sup>66</sup>

85. The World Economic Forum has also identified guiding principles for the industry based upon multistakeholder workshops, meetings of senior industry and public-sector leaders, and expert interviews, which include similarly-defined principles “consent,” and “control.”<sup>67</sup> Plaid’s conduct conflicts with these widely-recognized principles.

86. Plaid’s conduct also violates Plaid’s obligations under the GLBA (Section G.1). Plaid acknowledges these standards and its responsibilities under the GLBA (Section G.2), but, in practice, Plaid violates those standards along with consumers’ reasonable expectations founded thereupon (Section G.3). Furthermore, Plaid’s conduct and lack of disclosures fail to meet industry standards codified in California law (Section G.4). Plaid’s deceptive conduct and omissions are intentional.

### 1. The GLBA Standards

87. Plaid is a financial institution subject to the GLBA and the regulations promulgated thereunder, including Privacy of Consumer Financial Information (the “Privacy Rule”), 16 C.F.R. Part 313, recodified at 12 C.F.R. Part 1016 (“Reg. P”), and issued pursuant to the GLBA, 15 U.S.C. §§ 6801-6803. The Privacy Rule and Reg. P hold financial institutions to an elevated standard with regard to the privacy notices that must be provided to their customers.

Among other things:

a. Privacy notices must be “clear and conspicuous.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. “Clear and conspicuous means that a notice is reasonably

<sup>66</sup> See Nov. 21, 2019 Statement of American Bankers Association to House Financial Services Committee Task Force on Financial Technology, <https://www.aba.com/-/media/documents/testimonies-and-speeches/data-access-statement-for-the-record.pdf?rev=7cf1bb1d244d4de4a169fd2a1ce5da51>.

<sup>67</sup> See World Economic Forum, *The Appropriate Use of Customer Data in Financial Services* (Jan. 20, 2020), [http://www3.weforum.org/docs/WEF\\_FSIEG\\_Customer\\_Data\\_Preamble\\_And\\_Principles.pdf](http://www3.weforum.org/docs/WEF_FSIEG_Customer_Data_Preamble_And_Principles.pdf).

1 understandable and designed to call attention to the nature and significance of the information in  
2 the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1).

3 b. Privacy notices must “accurately reflect[.]” the financial institution’s privacy  
4 policies and practices. 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. The  
5 notices must include the categories of nonpublic personal information the financial institution  
6 collects and discloses, the categories of third parties to whom the financial institution discloses  
7 the information, and the financial institution’s security and confidentiality policies. 16 C.F.R.  
8 § 313.6; 12 C.F.R. § 1016.6.

9 c. Privacy notices must be provided “so that each consumer can reasonably be  
10 expected to receive actual notice.” 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. For the consumer who  
11 conducts transactions electronically, the financial institution must (1) “clearly and  
12 conspicuously” post the notice on an electronic site, and (2) “require the consumer to  
13 acknowledge receipt of the notice as a necessary step to obtaining a particular financial product  
14 or service.” 16 C.F.R. § 313.9(b)(1)(iii); 12 C.F.R. § 1016.9(b)(1)(iii).

15 88. Consistent with the requirements under the GLBA, the CFPB’s October 2017  
16 Consumer Protection Principles provide that the terms of access, storage, and use of consumer  
17 data must be “fully and effectively disclosed to the consumer, understood by the consumer, not  
18 overly broad, and consistent with the consumer’s reasonable expectations in light of the  
19 product(s) or service(s) selected by the consumer.” In addition, data access terms must address  
20 “access frequency, data scope, and retention period.” Further, consumers must be informed of any  
21 third parties that access or use their information, including the “identity and security of each such  
22 party, the data they access, their use of such data, and the frequency at which they access the  
23 data.”<sup>68</sup>

24  
25  
26  
27 <sup>68</sup> See Oct. 18, 2017 CFPB release: *Consumer Protection Principles: Consumer-Authorized*  
28 *Financial Data Sharing and Aggregation*,  
[https://files.consumerfinance.gov/f/documents/cfpb\\_consumer-protection-principles\\_data-aggregation.pdf](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

## 2. Plaid's Acknowledgement of Its Disclosure Obligations

89. Plaid is well aware of its disclosure obligations and has consistently held itself up as a paragon of consumer disclosure. For example, in an October 2016 publication, Plaid took the position that “[d]ata collection and retention policies should be clearly displayed in plain English to consumers by permissioned parties, typically during onboarding – in other words, *transparency is critical*.”<sup>69</sup>

90. Plaid has admitted its privacy policy is subject to the Privacy Rule’s “clear and conspicuous” requirement. Plaid also has recognized its responsibility for ensuring that the relevant privacy notices in the Participating Apps meet those requirements. For example, the 2016 version of Plaid’s “Legal” page pays lip-service to the requirements with the following statement in its developer-facing “Terms of Use”:

Your product must maintain a *clear and conspicuous link in its privacy policy to Plaid's Privacy Policy*. Such link must include a *clear and conspicuous statement* that each end user acknowledges and agrees that information will be treated in accordance with such policy. . . . All of the foregoing must be done in a form and manner that is acceptable to Plaid. You will immediately make any changes requested by us.<sup>70</sup>

91. Plaid similarly acknowledges that the data it transfers to the Participating Apps is subject to another aspect of the GLBA, the “Safeguards Rule” (16 C.F.R. Part 314). Plaid’s “Developer Policy” states: “Your systems and application(s) must handle End User Data securely. With respect to End User Data, you should follow industry best practices but, at a minimum, must . . . [c]omply with *relevant rules and regulations* with regard to the type of data you are handling, *such as the Safeguards Rule*.”<sup>71</sup>

92. In its February 2017 response to the CFPB’s RFI, Plaid stated:

An existing legal framework – the Gramm-Leach-Bliley Act (GLBA) – governs the proper disclosure and use of consumer financial data. Ecosystem participants – both traditional institutions

<sup>69</sup> See Oct. 2016 Plaid Publication: *Financial data access methods: Creating a balanced approach*, Appendix C to Plaid’s response to CFPB RFI, <https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf> (emphasis added).

<sup>70</sup> See <https://web.archive.org/web/20160920005638/https://plaid.com/legal/> (emphasis added).

<sup>71</sup> See <https://plaid.com/legal/>.



and newer digital players – should abide by this framework, including provisions that limit the use of permissioned data to the scope of the consumer’s consent. More generally, the disclosure and use of consumer data by digital products and services is subject to all applicable laws and regulations.

...

Beyond the letter of the law, both intermediaries and permissioned parties should also honor the principles of data minimization and consumer transparency. Consumers should know what data is being collected, and for how long it may be stored. . . . Permissioned parties and trusted intermediaries should clearly disclose terms of data collection policies to consumers.”<sup>72</sup>

93. In a March 2019 letter to the U.S. Senate, Plaid described its approach to data access as founded firmly in *affirmative consumer permission*:

Plaid represents a new approach enabled by modern technology, helping a consumer access their own data only when they chose to do so, and sharing it only with the companies they select. This is a consumer-permissioned model, in which consumers control what they do with their data.

Consumer permission is the backbone of account connectivity. However, industry disclosure practices can and should be improved. At Plaid, consumer permission and control are core principles. Unlike many other service providers who rely on personal or financial data, our account connectivity services require consumers to affirmatively provide or permission access to their account information to the company they want to share it with.

Most importantly, consumers should understand: What data is being shared? For what purpose? And what ability do they have to direct what happens to their data? At Plaid, we have developed simple, plain-English disclosures and privacy policies designed to help consumers understand which information is collected and how it is used, shared and stored. We have previously discussed the potential benefits of Schumer-box<sup>73</sup>-like disclosures for consumer data access, and believe Plaid—and the rest of the industry—should continue to develop and test more effective consumer disclosures.

[C]onsumer permission should be tied to the services the consumer requests or purposes for which they are specifically informed when

<sup>72</sup> See Feb. 21, 2017 Response by Plaid to CFPB’s Consumer Data Access RFI, <https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf> (emphasis added).

<sup>73</sup> A Schumer Box, named after Senator Chuck Schumer, is an easy-to-read table or “box” that discloses the rates, fees, terms and conditions of a credit card agreement as required under the federal Truth in Lending Act. It requires that all credit card companies use the same standardized format and font sizes to disclose certain aspects of a credit card agreement so consumers can easily understand and compare rates and fees associated with a credit card.



they grant access. Affirmative permission (not fine-print click-through) should be required in order to sell account data, even in aggregated form, to any parties the consumer doesn't have a direct permissioning relationship with. To do otherwise would breach the trust consumers place in fintech providers. Static disclosure, such as a Schumer box when initially seeking customer consent, is important. But ongoing control will require development of more dynamic controls, which should give consumers the ability to manage their data.<sup>74</sup>

In this letter, Plaid acknowledged: (a) how critically important it is for consumers to understand at the outset how their data is being accessed, used, shared, and stored; (b) the important role disclosures and privacy policies play in ensuring such understanding; (c) that consumer disclosures must be clear, plainly written, and easily understandable; (d) that consumer permission must be tied to the purpose for which they are granting access to their data; (e) that affirmative permission, and not "fine-print click-through," is the proper standard for obtaining consumer permission; (f) that static disclosures are not enough; and (g) that for static disclosures to be effective at all, they should mirror the form of the "Schumer box" used to disclose the terms for credit card agreements as mandated under the federal Truth in Lending Act.

94. Perret similarly has said that it is "really important" for consumers using Plaid's software to understand things like "data privacy, where their data is going, [and] how it's going."<sup>75</sup>

### **3. Violations of GLBA Standards in Plaid's Privacy Policy**

95. Plaid's acknowledgements of its responsibilities to consumers and obligations under the GLBA are not consistent with Plaid's actual practices. Plaid's privacy policy—accessible only in the small, greyed out hyperlink in Plaid's template consumer interface pictured above—is not meaningfully presented to Plaintiffs and Class members. Even if a consumer somehow became aware of the "policy," the privacy-related purported disclosures knowingly and intentionally violate the requirements of the Privacy Rule and Reg. P under the GLBA. By way of

<sup>74</sup> See Mar. 15, 2019 Letter from Plaid to U.S. Senate, [https://www.banking.senate.gov/imo/media/doc/Data%20Submission\\_Plaid1.pdf](https://www.banking.senate.gov/imo/media/doc/Data%20Submission_Plaid1.pdf).

<sup>75</sup> See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 21:38 to 26:11, <https://www.youtube.com/watch?v=sgnCs34mopw>.

1 example, Plaid's template presented to consumers, discussed and illustrated above with respect to  
 2 the Venmo app, violates these standards for the following reasons, without limitation:

3 a. Plaid's privacy policy is not "clear and conspicuous" because the text used in  
 4 Plaid's software to link to its privacy policy (the "prompting text") is not "designed to call  
 5 attention" to the existence of the notice itself. 16 C.F.R. § 313.3(b)(1). Plaid failed to meet that  
 6 standard because, among other reasons, it (a) did not "[u]se a plain-language heading to call  
 7 attention to the notice," but rather simply included a link in a sentence above the "Continue"  
 8 button (16 C.F.R. § 313.3(b)(2)(ii)(A)); (b) did not "[u]se a typeface and type size that are easy  
 9 to read," but rather used the smallest and lightest font on the screen (16 C.F.R.  
 10 § 313.3(b)(2)(ii)(B)); (c) did not "[u]se boldface or italics for key words," but rather made the  
 11 hyperlink the same font as the surrounding text (16 C.F.R. § 313.3(b)(2)(ii)(D)); and (d) did not  
 12 "use distinctive type size, style, and graphic devices, such as shading or sidebars," when  
 13 combining its notice with other information. 16 C.F.R. § 313.3(b)(2)(ii)(E).

14 b. Plaid's privacy policy is not "clear and conspicuous" because the prompting text  
 15 is not "designed to call attention" to the "nature and significance of the information" in the  
 16 notice. 16 C.F.R. § 313.3(b)(1). Plaid failed to meet that standard because nothing in the  
 17 prompting text calls attention to the nature or significance of the information in the notice. That  
 18 screen of Plaid's software contains no indication, for example, that Plaid is a third party; that  
 19 Plaid will collect the user's private bank login information itself; or, critically, that Plaid will  
 20 access, collect, transfer, sell, use, or store the entirety of personal information available from the  
 21 user's bank, including years of transactional banking data from all linked accounts. Plaid was  
 22 required to make that information "reasonably understandable" by, for example, presenting the  
 23 information in "clear, concise sentences." 16 C.F.R. § 313.3(b)(2)(i)(A).

24 c. Plaid's privacy policy is not "clear and conspicuous" because the policy is not  
 25 "designed to call attention" to the "nature and significance of the information" therein. 16 C.F.R.  
 26 § 313.3(b)(1). Among other things, Plaid's privacy policy fails to explain that Plaid will access,  
 27 collect, transfer, sell, use, or store the entirety of personal information available from the user's  
 28 bank, including years of transactional banking data from all linked accounts. In addition, by

1 using non-specific, misleading statements about Plaid collecting “transactional information,”  
 2 Plaid fails to “[a]void explanations that are imprecise and readily subject to different  
 3 interpretations.” 16 C.F.R. § 313.3(b)(2)(i)(F).

4 d. Plaid’s privacy policy is not “clear and conspicuous” because the prompting text  
 5 is not placed on a screen in the Venmo app (or any Participating App) that consumers  
 6 “frequently access,” and—for the reasons described above—is not “labeled appropriately to  
 7 convey the importance, nature and relevance of the notice.” 16 C.F.R. § 313.3(b)(2)(iii). In  
 8 addition, Plaid’s screen is not designed to ensure that other elements “do not distract from the  
 9 notice.” *Id.*

10 e. Plaid’s privacy policy does not “accurately reflect[]” its actual policies and  
 11 practices. 16 C.F.R. §§ 313.4 and 313.5. Plaid’s privacy policy fails to explain that Plaid will  
 12 access, collect, transfer, sell, use, or store the entirety of personal information available from the  
 13 user’s bank, including years of transactional banking data from all linked accounts. Rather, by  
 14 using non-specific, misleading statements about Plaid collecting “transactional information,”  
 15 Plaid obscures the true nature of its practices.

16 f. Plaid’s privacy policy is not provided “so that each consumer can reasonably be  
 17 expected to receive actual notice.” 16 C.F.R. § 313.9. As discussed above, Plaid did not “clearly  
 18 and conspicuously” post its policy for its users, all of whom conduct transactions electronically.  
 19 16 C.F.R. § 313.9(b)(1)(iii). Neither does Plaid “require the consumer to acknowledge receipt of  
 20 the notice as a necessary step to obtaining a particular financial product or service.” *Id.*

#### 21 4. Violations of CalFIPA and CalOPPA Standards in Plaid’s Privacy 22 Policy

23 96. CalFIPA requires that the language in privacy policies be “designed to call  
 24 attention to the nature and significance of the information” therein, use “short explanatory  
 25 sentences,” and “avoid[] explanations that are imprecise or readily subject to different  
 26 interpretations.” Cal. Fin. Code § 4053(d)(1). The text must be no smaller than 10-point type and  
 27 “use[] boldface or italics for key words.” *Id.* In passing CalFIPA, the California legislature  
 28 explicitly provided that its intent was “to afford persons greater privacy protections than those

provided in . . . the federal Gramm-Leach-Bliley Act, and that this division be interpreted to be consistent with that purpose.” Cal. Fin. Code § 4051.

97. CalOPPA requires that “[a]n operator of a[n] . . . online service that collects personally identifiable information through the Internet about individual consumers” must “[i]dentify the categories of personally identifiable information that the operator collects . . . about individual consumers who use or visit its . . . online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.” Cal. Bus. & Prof. Code § 22575. It also requires that an operator of any online service, as defined therein, “conspicuously post” its privacy policy. *Id.* It defines “conspicuously post” to require a text hyperlink to the policy that includes the word “privacy”; is “written in capital letters equal to or greater in size than the surrounding text”; “is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.” Cal. Bus. Prof. Code § 22577(b).

98. For the same reasons that Plaid’s privacy policy violates the standards set forth elsewhere in this complaint, Plaid’s privacy policy fails to provide the additional protections required by California law.

## **VI. INJURY AND DAMAGES TO THE CLASS**

99. As Participating App users who linked their financial accounts using Plaid’s software integrated with the app, Plaintiffs and all other Class members have suffered egregious invasions of privacy, violations of their dignitary rights, and significant economic damages as a direct result of Plaid’s misconduct.

### **A. The Named Plaintiffs’ Experiences**

100. Plaintiff **Carrie Anderson** signed up to use the Venmo app in or about 2019, and the Cash App app in or about February 2020, via her mobile phone. When Ms. Anderson established her accounts with Venmo and Cash App, she did so for the purpose, consistent with the services offered by Venmo and Cash App, of being able to send and receive payments to or from friends, acquaintances, and other consumers.

1           101. To the extent Ms. Anderson recalls specific details regarding the process of  
2 logging into her bank account in the Venmo and Cash App apps so that she could send and  
3 receive money through the apps, those details are consistent with the discussion of Plaid's  
4 interface herein. Ms. Anderson does not recall being prompted to read any privacy policy from  
5 Plaid during the process of logging into her bank account and does not recall having ever read any  
6 privacy policy from Plaid when she linked her bank account.

7           102. At the time Ms. Anderson established her accounts with Venmo and Cash App,  
8 she was not aware of the existence or role of Plaid. When she was prompted in the Venmo and  
9 Cash App apps to log into her bank account, she believed she was doing so through an official  
10 connection with her bank. She was unaware that she was providing her login credentials to Plaid.

11           103. When Ms. Anderson was prompted in the Venmo and Cash App apps to log into  
12 her bank account, she was not aware that Plaid: (a) would collect any of her banking information  
13 as part of that process; (b) would collect, receive, or store any of her banking information beyond  
14 that which was strictly necessary to effectuate transfer or receipt of payments from or to her bank  
15 account; (c) would collect, receive, or store any transaction-related banking information beyond  
16 the specific transactions she triggered using the Venmo and Cash App apps; (d) would sell her  
17 banking data to Venmo and Cash App; or (e) would use or monetize her banking data in any way.  
18 On the contrary, Ms. Anderson reasonably expected that such conduct would not occur.

19           104. By logging into her bank account when prompted in the Venmo and Cash App  
20 apps, Ms. Anderson intended only to prompt her bank to provide Venmo and Cash App with a  
21 connection to her account for the limited purposes of withdrawing funds for transfers she  
22 triggered in the Venmo and Cash App accounts and depositing funds for transfers other Venmo  
23 and Cash App users made to her.

24           105. If Ms. Anderson had learned what she now knows about the existence and role of  
25 Plaid, or the practices of Plaid in collecting, receiving, storing, selling, or using her banking data,  
26 she would not have connected her bank account in the Venmo and Cash App apps the way she  
27 did.  
28

1           106. Since the time Ms. Anderson established her accounts with Venmo and Cash App,  
2 she has used the apps sparingly.

3           107. Ms. Anderson is informed and believes that Plaid: (a) collected her private bank  
4 login credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed her  
5 private banking information and data; (c) sold her private banking information to Venmo and  
6 Cash App; and (d) monetized her private banking data by performing analytics on it and using it  
7 to develop value-added products for Plaid's customers. Ms. Anderson did not and does not  
8 consent to these activities.

9           108. Ms. Anderson has suffered actual and concrete injury as a result of Plaid's  
10 misconduct, including, *inter alia*, economic damages caused by the misappropriation of her  
11 sensitive financial and personal data, and harm to her dignitary rights and interests as a human  
12 being related to unauthorized parties accessing, storing, selling, and using her most private  
13 financial information and intruding upon her private affairs and concerns. She is also at increased  
14 risk of identity theft and fraud and regularly monitors her credit, bank, and other account  
15 statements for evidence of identity theft and fraud. She anticipates continuing to do so for the  
16 foreseeable future.

17           109. Ms. Anderson's financial account at TD Bank was "linked" to and verified for use  
18 with the Venmo and Cash App apps. Ms. Anderson has used TD Bank's password-protected  
19 interface with its servers and systems to receive communications about her financial account,  
20 including without limitation bank statements addressed to her and a listing of her recent account  
21 activity, as well as messages, notifications, and other transfers of information.

22           110. In addition, Ms. Anderson has opened a bank account for her minor child. This  
23 account is associated with Ms. Anderson's account and accessible with Ms. Anderson's TD Bank  
24 username and password; thus, pursuant to the application of Plaid's policies, this minor  
25 individual's account was accessed by Plaid repeatedly and without authorization.

26           111. Plaintiff **James Cottle** signed up to use the Venmo app in or about January 2019,  
27 via his mobile phone. When Mr. Cottle established his account with Venmo, he did so for the  
28

1 purpose, consistent with the services offered by Venmo, of being able to send and receive  
2 payments to or from friends, acquaintances, and other consumers.

3 112. To the extent Mr. Cottle recalls specific details about the process of linking his  
4 bank account to his Venmo account so that he could send and receive money through the app,  
5 those details are consistent with the discussion of Plaid's interface herein. Mr. Cottle does not  
6 recall being prompted to read any privacy policy from Plaid during the process of logging into his  
7 bank account and does not recall having ever read any privacy policy from Plaid when he linked  
8 his bank account.

9 113. At the time Mr. Cottle established his account with Venmo, he was not aware of  
10 the existence or role of Plaid. When he was prompted in the Venmo app to log into his bank  
11 account, he believed he was doing so through an official connection with his bank. He was  
12 unaware that he was providing his login credentials to Plaid.

13 114. When Mr. Cottle was prompted in the Venmo app to log into his bank account, he  
14 was not aware that Plaid: (a) would collect any of his banking information as part of that process;  
15 (b) would collect, receive, or store any of his banking information beyond that which was strictly  
16 necessary to effectuate transfer or receipt of payments from or to his bank account; (c) would  
17 collect, receive, or store any transaction-related banking information beyond the specific  
18 transactions he triggered using the Venmo app; (d) would sell his banking data to Venmo; or  
19 (e) would use or monetize his banking data in any way. On the contrary, Mr. Cottle reasonably  
20 expected that such conduct would not occur.

21 115. By logging into his bank account when prompted in the Venmo app, Mr. Cottle  
22 intended only to prompt his bank to provide Venmo with a connection to his account for the  
23 limited purposes of withdrawing funds for transfers he triggered in the Venmo account and  
24 depositing funds for transfers other Venmo users made to him.

25 116. If Mr. Cottle had learned what he now knows about the existence and role of Plaid,  
26 or the practices of Plaid in collecting, receiving, storing, selling, or using his banking data, he  
27 would not have connected his bank account in the Venmo app the way he did.  
28

1           117. Mr. Cottle is informed and believes that Plaid: (a) collected his private bank login  
2 credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed his private  
3 banking information and data; (c) sold his private banking information to Venmo; and  
4 (d) monetized his private banking data by performing analytics on it and using it to develop  
5 value-added products for Plaid's customers. Mr. Cottle did not and does not consent to these  
6 activities.

7           118. Mr. Cottle has suffered actual and concrete injury as a result of Plaid's  
8 misconduct, including, *inter alia*, economic damages caused by the misappropriation of his  
9 sensitive financial and personal data, and harm to his dignitary rights and interests as a human  
10 being related to unauthorized parties accessing, storing, selling, and using his most private  
11 financial information and intruding upon his private affairs and concerns. He is also at increased  
12 risk of identity theft and fraud and regularly monitors his credit, bank, and other account  
13 statements for evidence of identity theft and fraud. He anticipates continuing to do so for the  
14 foreseeable future.

15           119. Mr. Cottle's financial account at Wells Fargo Bank was "linked" to and verified  
16 for use with the Venmo app. Mr. Cottle has used Wells Fargo's password-protected interface with  
17 its servers and systems to receive communications about his financial account, including without  
18 limitation bank statements addressed to him and a listing of his recent account activity, as well as  
19 messages, notifications, and other transfers of information.

20           120. In addition, Mr. Cottle has opened a bank account for his minor child. This  
21 account is associated with Mr. Cottle's accounts and accessible with Mr. Cottle's Wells Fargo  
22 Bank username and password; thus, pursuant to the application of Plaid's policies, this minor  
23 individual's account was accessed by Plaid repeatedly and without authorization.

24           121. Plaintiff **Rachel Curtis** signed up to use the Venmo app in or about April 2015,  
25 via her mobile phone. When Ms. Curtis established her account with Venmo, she did so for the  
26 purpose, consistent with the services offered by Venmo, of being able to send and receive  
27 payments to or from friends, acquaintances, and other consumers.  
28



1           122. To the extent Ms. Curtis recalls specific details regarding the process of logging  
2 into her bank account in the Venmo app so that she could send and receive money through the  
3 app, those details are consistent with the discussion of Plaid's interface herein. Ms. Curtis does  
4 not recall being prompted to read any privacy policy from Plaid during the process of logging into  
5 her bank account and does not recall having ever read any privacy policy from Plaid when she  
6 linked her bank account.

7           123. At the time Ms. Curtis established her account with Venmo, she was not aware of  
8 the existence or role of Plaid. When she was prompted in the Venmo app to log into her bank  
9 account, she believed she was doing so through an official connection with her bank. She was  
10 unaware that she was providing her login credentials to Plaid.

11           124. When Ms. Curtis was prompted in the Venmo app to log into her bank account,  
12 she was not aware that Plaid: (a) would collect any of her banking information as part of that  
13 process; (b) would collect, receive, or store any of her banking information beyond that which  
14 was strictly necessary to effectuate transfer or receipt of payments from or to her bank account;  
15 (c) would collect, receive, or store any transaction-related banking information beyond the  
16 specific transactions she triggered using the Venmo app; (d) would sell her banking data to  
17 Venmo; or (e) would use or monetize her banking data in any way. On the contrary, Ms. Curtis  
18 reasonably expected that such conduct would not occur.

19           125. By logging into her bank account when prompted in the Venmo app, Ms. Curtis  
20 intended only to prompt her bank to provide Venmo with a connection to her account for the  
21 limited purposes of withdrawing funds for transfers she triggered in the Venmo account and  
22 depositing funds for transfers other Venmo users made to her.

23           126. If Ms. Curtis had learned what she now knows about the existence and role of  
24 Plaid, or the practices of Plaid in collecting, receiving, storing, selling, or using her banking data,  
25 she would not have connected her bank account in the Venmo app the way she did.

26           127. Ms. Curtis is informed and believes that Plaid: (a) collected her private bank login  
27 credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed her private  
28 banking information and data; (c) sold her private banking information to Venmo; and

1 (d) monetized her private banking data by performing analytics on it and using it to develop  
2 value-added products for Plaid's customers. Ms. Curtis did not and does not consent to these  
3 activities.

4 128. Ms. Curtis has suffered actual and concrete injury as a result of Plaid's  
5 misconduct, including, *inter alia*, economic damages caused by the misappropriation of her  
6 sensitive financial and personal data, and harm to her dignitary rights and interests as a human  
7 being related to unauthorized parties accessing, storing, selling, and using her most private  
8 financial information and intruding upon her private affairs and concerns. She is also at increased  
9 risk of identity theft and fraud and regularly monitors her credit, bank, and other account  
10 statements for evidence of identity theft and fraud. She anticipates continuing to do so for the  
11 foreseeable future.

12 129. Ms. Curtis's financial account at USAA Bank was "linked" to and verified for use  
13 with the Venmo app. Ms. Curtis has used password-protected interfaces with USAA Bank's  
14 servers and systems to receive communications about her financial account, including without  
15 limitation bank statements addressed to her and a listing of her recent account activity, as well as  
16 messages, notifications, and other transfers of information.

17 130. Plaintiff **David Evans** signed up to use the Venmo app in or about summer of  
18 2016, via his mobile phone. When Mr. Evans established his account with Venmo, he did so for  
19 the purpose, consistent with the services offered by Venmo, of being able to send and receive  
20 payments to or from friends, acquaintances, and other consumers.

21 131. To the extent Mr. Evans recalls specific details about the process of linking his  
22 bank account to his Venmo account so that he could send and receive money through the app,  
23 those details are consistent with the discussion of Plaid's interface herein. Mr. Evans does not  
24 recall being prompted to read any privacy policy from Plaid during the process of logging into his  
25 bank account and does not recall having ever read any privacy policy from Plaid when he linked  
26 his bank account.

27 132. At the time Mr. Evans established his account with Venmo and at the time he  
28 linked his bank account using the instant verification process, he was not aware of the existence

1 or role of Plaid. When he was prompted in the Venmo app to log into his bank account, he  
2 believed he was doing so through an official connection with his bank. He was unaware that he  
3 was providing his login credentials to Plaid.

4 133. When Mr. Evans was prompted in the Venmo app to log into his bank account, he  
5 was not aware that Plaid: (a) would collect any of his banking information as part of that process;  
6 (b) would collect, receive, or store any of his banking information beyond that which was strictly  
7 necessary to effectuate transfer or receipt of payments from or to his bank account; (c) would  
8 collect, receive, or store any transaction-related banking information beyond the specific  
9 transactions he triggered using the Venmo app; (d) would sell his banking data to Venmo; or  
10 (e) would use or monetize his banking data in any way. On the contrary, Mr. Evans reasonably  
11 expected that such conduct would not occur.

12 134. By logging into his bank account when prompted in the Venmo app, Mr. Evans  
13 intended only to prompt his bank to provide Venmo with a connection to his account for the  
14 limited purposes of withdrawing funds for transfers he triggered in the Venmo account and  
15 depositing funds for transfers other Venmo users made to him.

16 135. If Mr. Evans had learned what he now knows about the existence and role of Plaid,  
17 or the practices of Plaid in collecting, receiving, storing, selling, or using his banking data, he  
18 would not have connected his bank account in the Venmo app the way he did.

19 136. Since the time Evans established his account with Venmo, he has used the app  
20 sparingly.

21 137. Mr. Evans is informed and believes that Plaid: (a) collected his private bank login  
22 credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed his private  
23 banking information and data; (c) sold his private banking information to Venmo; and  
24 (d) monetized his private banking data by performing analytics on it and using it to develop  
25 value-added products for Plaid's customers. Mr. Evans did not and does not consent to these  
26 activities.

27 138. Mr. Evans has suffered actual and concrete injury as a result of Plaid's  
28 misconduct, including, *inter alia*, economic damages caused by the misappropriation of his

1 sensitive financial and personal data, and harm to his dignitary rights and interests as a human  
2 being related to unauthorized parties accessing, storing, selling, and using his most private  
3 financial information and intruding upon his private affairs and concerns. He is also at increased  
4 risk of identity theft and fraud and monitors his credit, bank, and other account statements on  
5 almost a daily basis for evidence of identity theft and fraud. He anticipates continuing to do so for  
6 the foreseeable future.

7 139. Mr. Evans's financial account at UMe Federal Credit Union was "linked" to and  
8 verified for use with the Venmo app. Mr. Evans has used UMe's password-protected interface  
9 with its servers and systems to receive communications about his financial account, including  
10 without limitation bank statements addressed to him and a listing of his recent account activity, as  
11 well as messages, notifications, and other transfers of information.

12 140. Plaintiff **Logan Mitchell** signed up to use the Venmo app on or about August 15,  
13 2015, and the Cash App app on or about September 1, 2015, via her mobile phone. When Ms.  
14 Mitchell established her accounts with Venmo and Cash App, she did so for the purpose,  
15 consistent with the services offered by Venmo and Cash App, of being able to send and receive  
16 payments to or from friends, acquaintances, businesses, and other consumers.

17 141. To the extent Ms. Mitchell recalls specific details regarding the process of logging  
18 into her bank account in the Venmo and Cash App apps so that she could send and receive money  
19 through the apps, those details are consistent with the discussion of Plaid's interface herein. Ms.  
20 Mitchell does not recall being prompted to read any privacy policy from Plaid during the process  
21 of logging into her bank account and does not recall having ever read any privacy policy from  
22 Plaid when she linked her bank account.

23 142. At the time Ms. Mitchell established her accounts with Venmo and Cash App, she  
24 was not aware of the existence or role of Plaid. When she was prompted in the Venmo and Cash  
25 App apps to log into her bank account, she believed she was doing so through an official  
26 connection with her bank. She was unaware that she was providing her login credentials to Plaid.

27 143. When Ms. Mitchell was prompted in the Venmo and Cash App apps to log into her  
28 bank account, she was not aware that Plaid: (a) would collect any of her banking information as

1 part of that process; (b) would collect, receive, or store any of her banking information beyond  
2 that which was strictly necessary to effectuate transfer or receipt of payments from or to her bank  
3 account; (c) would collect, receive, or store any transaction-related banking information beyond  
4 the specific transactions she triggered using the Venmo and Cash App apps; (d) would sell her  
5 banking data to Venmo and Cash App; or (e) would use or monetize her banking data in any way.  
6 On the contrary, Ms. Mitchell reasonably expected that such conduct would not occur.

7 144. By logging into her bank account when prompted in the Venmo and Cash App  
8 apps, Ms. Mitchell intended only to prompt her bank to provide Venmo and Cash App with a  
9 connection to her account for the limited purposes of withdrawing funds for transfers she  
10 triggered in the Venmo and Cash App accounts and depositing funds for transfers other Venmo  
11 and Cash App users made to her.

12 145. If Ms. Mitchell had learned what she now knows about the existence and role of  
13 Plaid, or the practices of Plaid in collecting, receiving, storing, selling, or using her banking data,  
14 she would not have connected her bank account in the Venmo and Cash App apps the way she  
15 did.

16 146. Since the time Ms. Mitchell established her account with Cash App, she has used  
17 the app sparingly.

18 147. Ms. Mitchell is informed and believes that Plaid: (a) collected her private bank  
19 login credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed her  
20 private banking information and data; (c) sold her private banking information to Venmo and  
21 Cash App; and (d) monetized her private banking data by performing analytics on it and using it  
22 to develop value-added products for Plaid's customers. Ms. Mitchell did not and does not consent  
23 to these activities.

24 148. Ms. Mitchell has suffered actual and concrete injury as a result of Plaid's  
25 misconduct, including, *inter alia*, economic damages caused by the misappropriation of her  
26 sensitive financial and personal data, and harm to her dignitary rights and interests as a human  
27 being related to unauthorized parties accessing, storing, selling, and using her most private  
28 financial information and intruding upon her private affairs and concerns. She is also at increased

1 risk of identity theft and fraud and regularly monitors her credit, bank, and other account  
2 statements for evidence of identity theft and fraud. She anticipates continuing to do so for the  
3 foreseeable future.

4 149. Ms. Mitchell's financial account at Chase Bank was "linked" to and verified for  
5 use with the Venmo and Cash App apps. Ms. Mitchell's financial account at California Coast  
6 Credit Union was also "linked" to and verified for use with the Venmo app. Ms. Mitchell has  
7 used Chase Bank's and California Coast Credit Union's password-protected interfaces with their  
8 servers and systems to receive communications about her financial accounts, including without  
9 limitation bank statements addressed to her and a listing of her recent account activity, as well as  
10 messages, notifications, and other transfers of information.

11 150. Plaintiff **Alexis Mullen** signed up to use the Venmo app in or about March 2014,  
12 via her personal computer. When Ms. Mullen established her account with Venmo, she did so for  
13 the purpose, consistent with the services offered by Venmo, of being able to send and receive  
14 payments to or from friends, acquaintances, and other consumers.

15 151. To the extent Ms. Mullen recalls specific details regarding the process of logging  
16 into her bank accounts in the Venmo app so that she could send and receive money through the  
17 app, those details are consistent with the discussion of Plaid's interface herein. Ms. Mullen does  
18 not recall being prompted to read any privacy policy from Plaid during the process of logging into  
19 her bank accounts and does not recall having ever read any privacy policy from Plaid when she  
20 linked her bank accounts.

21 152. At the time Ms. Mullen established her account with Venmo, she was not aware of  
22 the existence or role of Plaid. When she was prompted in the Venmo app to log into her bank  
23 accounts, she believed she was doing so through an official connection with her banks. She was  
24 unaware that she was providing her login credentials to Plaid.

25 153. When Ms. Mullen was prompted in the Venmo app to log into her bank accounts,  
26 she was not aware that Plaid: (a) would collect any of her banking information as part of that  
27 process; (b) would collect, receive, or store any of her banking information beyond that which  
28 was strictly necessary to effectuate transfer or receipt of payments from or to her bank accounts;

1 (c) would collect, receive, or store any transaction-related banking information beyond the  
2 specific transactions she triggered using the Venmo app; (d) would sell her banking data to  
3 Venmo; or (e) would use or monetize her banking data in any way. On the contrary, Ms. Mullen  
4 reasonably expected that such conduct would not occur.

5 154. By logging into her bank accounts when prompted in the Venmo app, Ms. Mullen  
6 intended only to prompt her banks to provide Venmo with a connection to her account for the  
7 limited purposes of withdrawing funds for transfers she triggered in the Venmo account and  
8 depositing funds for transfers other Venmo users made to her.

9 155. If Ms. Mullen had learned what she now knows about the existence and role of  
10 Plaid, or the practices of Plaid in collecting, receiving, storing, selling, or using her banking data,  
11 she would not have connected her bank account in the Venmo app the way she did.

12 156. Ms. Mullen is informed and believes that Plaid: (a) collected her private bank  
13 login credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed her  
14 private banking information and data; (c) sold her private banking information to Venmo; and  
15 (d) monetized her private banking data by performing analytics on it and using it to develop  
16 value-added products for Plaid's customers. Ms. Mullen did not and does not consent to these  
17 activities.

18 157. Ms. Mullen has suffered actual and concrete injury as a result of Plaid's  
19 misconduct, including, *inter alia*, economic damages caused by the misappropriation of her  
20 sensitive financial and personal data, and harm to her dignitary rights and interests as a human  
21 being related to unauthorized parties accessing, storing, selling, and using her most private  
22 financial information and intruding upon her private affairs and concerns. She is also at increased  
23 risk of identity theft and fraud and regularly monitors her credit, bank, and other account  
24 statements for evidence of identity theft and fraud. She anticipates continuing to do so for the  
25 foreseeable future.

26 158. Ms. Mullen's financial accounts at TD Bank and PNC Bank were "linked" to and  
27 verified for use with the Venmo app. Ms. Mullen has used password-protected interfaces with  
28 both financial institutions' servers and systems to receive communications about her financial

1 accounts, including without limitation bank statements addressed to her and a listing of her recent  
2 account activity, as well as messages, notifications, and other transfers of information.

3 159. Plaintiff **Jordan Sacks** signed up to use the Venmo app in or about June 2014, via  
4 his personal computer. When Mr. Sacks established his account with Venmo, he did so for the  
5 purpose, consistent with the services offered by Venmo, of being able to send and receive  
6 payments to or from friends, acquaintances, and other consumers.

7 160. To the extent Mr. Sacks recalls specific details about the process of linking his  
8 bank account to his Venmo account so that he could send and receive money through the app,  
9 those details are consistent with the discussion of Plaid's interface herein. Mr. Sacks does not  
10 recall being prompted to read any privacy policy from Plaid during the process of logging into his  
11 bank account and does not recall having ever read any privacy policy from Plaid when he linked  
12 his bank account.

13 161. At the time Mr. Sacks established his account with Venmo, he was not aware of  
14 the existence or role of Plaid. When he was prompted in the Venmo app to log into his bank  
15 account, he believed he was doing so through an official connection with his bank. He was  
16 unaware that he was providing his login credentials to Plaid.

17 162. When Mr. Sacks was prompted in the Venmo app to log into his bank account, he  
18 was not aware that Plaid: (a) would collect any of his banking information as part of that process;  
19 (b) would collect, receive, or store any of his banking information beyond that which was strictly  
20 necessary to effectuate transfer or receipt of payments from or to his bank account; (c) would  
21 collect, receive, or store any transaction-related banking information beyond the specific  
22 transactions he triggered using the Venmo app; (d) would sell his banking data to Venmo; or  
23 (e) would use or monetize his banking data in any way. On the contrary, Mr. Sacks reasonably  
24 expected that such conduct would not occur.

25 163. By logging into his bank account when prompted in the Venmo app, Mr. Sacks  
26 intended only to prompt his bank to provide Venmo with a connection to his account for the  
27 limited purposes of withdrawing funds for transfers he triggered in the Venmo account and  
28 depositing funds for transfers other Venmo users made to him.



1           164. If Mr. Sacks had learned what he now knows about the existence and role of Plaid,  
2 or the practices of Plaid in collecting, receiving, storing, selling, or using his banking data, he  
3 would not have connected his bank account in the Venmo app the way he did.

4           165. Mr. Sacks is informed and believes that Plaid: (a) collected his private bank login  
5 credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed his private  
6 banking information and data; (c) sold his private banking information to Venmo; and  
7 (d) monetized his private banking data by performing analytics on it and using it to develop  
8 value-added products for Plaid's customers. Mr. Sacks did not and does not consent to these  
9 activities.

10           166. Mr. Sacks has suffered actual and concrete injury as a result of Plaid's misconduct,  
11 including, *inter alia*, economic damages caused by the misappropriation of his sensitive financial  
12 and personal data, and harm to his dignitary rights and interests as a human being related to  
13 unauthorized parties accessing, storing, selling, and using his most private financial information  
14 and intruding upon his private affairs and concerns. He is also at increased risk of identity theft  
15 and fraud and regularly monitors his credit, bank, and other account statements for evidence of  
16 identity theft and fraud. He anticipates continuing to do so for the foreseeable future.

17           167. Mr. Sacks's financial account at Chase Bank was "linked" to and verified for use  
18 with the Venmo app. Mr. Sacks has used Chase Bank's password-protected interface with its  
19 servers and systems to receive communications about his financial account, including without  
20 limitation bank statements addressed to him and a listing of his recent account activity, as well as  
21 messages, notifications, and other transfers of information.

22           168. Plaintiff **Frederick Schoeneman** signed up to use the Venmo app on or about July  
23 15, 2016, via his mobile phone. When Mr. Schoeneman established his account with Venmo, he  
24 did so for the purpose, consistent with the services offered by Venmo, of being able to send and  
25 receive payments to or from vendors, friends, acquaintances, and other consumers.

26           169. To the extent Mr. Schoeneman recalls specific details about the process of linking  
27 his bank account to his Venmo account so that he could send and receive money through the app,  
28 those details are consistent with the discussion of Plaid's interface herein. Mr. Schoeneman does

1 not recall being prompted to read any privacy policy from Plaid during the process of logging into  
2 his bank account and does not recall having ever read any privacy policy from Plaid when he  
3 linked his bank account.

4 170. At the time Mr. Schoeneman established his account with Venmo, he was not  
5 aware of the existence or role of Plaid. When he was prompted in the Venmo app to log into his  
6 bank account, he believed he was doing so through an official connection with his bank. He was  
7 unaware that he was providing his login credentials to Plaid.

8 171. When Mr. Schoeneman was prompted in the Venmo app to log into his bank  
9 account, he was not aware that Plaid: (a) would collect any of his banking information as part of  
10 that process; (b) would collect, receive, or store any of his banking information beyond that which  
11 was strictly necessary to effectuate transfer or receipt of payments from or to his bank account;  
12 (c) would collect, receive, or store any transaction-related banking information beyond the  
13 specific transactions he triggered using the Venmo app; (d) would sell his banking data to  
14 Venmo; or (e) would use or monetize his banking data in any way. On the contrary, Mr.  
15 Schoeneman reasonably expected that such conduct would not occur.

16 172. By logging into his bank account when prompted in the Venmo app, Mr.  
17 Schoeneman intended only to prompt his bank to provide Venmo with a connection to his account  
18 for the limited purposes of withdrawing funds for transfers he triggered in the Venmo account and  
19 depositing funds for transfers other Venmo users made to him.

20 173. If Mr. Schoeneman had learned what he now knows about the existence and role  
21 of Plaid, or the practices of Plaid in collecting, receiving, storing, selling, or using his banking  
22 data, he would not have connected his bank account in the Venmo app the way he did.

23 174. Since the time Mr. Schoeneman established his account with Venmo, he has used  
24 the app sparingly.

25 175. Mr. Schoeneman is informed and believes that Plaid: (a) collected his private bank  
26 login credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed his  
27 private banking information and data; (c) sold his private banking information to Venmo; and  
28 (d) monetized his private banking data by performing analytics on it and using it to develop

1 value-added products for Plaid's customers. Mr. Schoeneman did not and does not consent to  
2 these activities.

3 176. Mr. Schoeneman has suffered actual and concrete injury as a result of Plaid's  
4 misconduct, including, *inter alia*, economic damages caused by the misappropriation of his  
5 sensitive financial and personal data, and harm to his dignitary rights and interests as a human  
6 being related to unauthorized parties accessing, storing, selling, and using his most private  
7 financial information and intruding upon his private affairs and concerns. He is also at increased  
8 risk of identity theft and fraud and regularly monitors his credit, bank, and other account  
9 statements for evidence of identity theft and fraud. He anticipates continuing to do so for the  
10 foreseeable future.

11 177. Mr. Schoeneman's financial account at Wells Fargo Bank was "linked" to and  
12 verified for use with the Venmo app. Mr. Schoeneman has used Wells Fargo Bank's password-  
13 protected interface with its servers and systems to receive communications about his financial  
14 account, including without limitation bank statements addressed to him and a listing of his recent  
15 account activity, as well as messages, notifications, and other transfers of information.

16 178. Plaintiff **Gabriel Sotelo** signed up to use the Venmo app in or about February or  
17 March 2020, via his mobile phone. When Mr. Sotelo established his account with Venmo, he did  
18 so for the purpose, consistent with the services offered by Venmo, of being able to send and  
19 receive payments to or from friends, acquaintances, and other consumers.

20 179. To the extent Mr. Sotelo recalls specific details about the process of linking his  
21 bank account to his Venmo account so that he could send and receive money through the app,  
22 those details are consistent with the discussion of Plaid's interface herein. Mr. Sotelo does not  
23 recall being prompted to read any privacy policy from Plaid during the process of logging into his  
24 bank account and does not recall having ever read any privacy policy from Plaid when he linked  
25 his bank account.

26 180. At the time Mr. Sotelo established his account with Venmo, he was not aware of  
27 the existence or role of Plaid. When he was prompted in the Venmo app to log into his bank  
28

1 account, he believed he was doing so through an official connection with his bank. He was  
2 unaware that he was providing his login credentials to Plaid.

3 181. When Mr. Sotelo was prompted in the Venmo app to log into his bank account, he  
4 was not aware that Plaid: (a) would collect any of his banking information as part of that process;  
5 (b) would collect, receive, or store any of his banking information beyond that which was strictly  
6 necessary to effectuate transfer or receipt of payments from or to his bank account; (c) would  
7 collect, receive, or store any transaction-related banking information beyond the specific  
8 transactions he triggered using the Venmo app; (d) would sell his banking data to Venmo; or  
9 (e) would use or monetize his banking data in any way. On the contrary, Mr. Sotelo reasonably  
10 expected that such conduct would not occur.

11 182. By logging into his bank account when prompted in the Venmo app, Mr. Sotelo  
12 intended only to prompt his bank to provide Venmo with a connection to his account for the  
13 limited purposes of withdrawing funds for transfers he triggered in the Venmo account and  
14 depositing funds for transfers other Venmo users made to him.

15 183. If Mr. Sotelo had learned what he now knows about the existence and role of  
16 Plaid, or the practices of Plaid in collecting, receiving, storing, selling, or using his banking data,  
17 he would not have connected his bank account in the Venmo app the way he did.

18 184. Since the time Mr. Sotelo established his account with Venmo, he has used the app  
19 sparingly.

20 185. Mr. Sotelo is informed and believes that Plaid: (a) collected his private bank login  
21 credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed his private  
22 banking information and data; (c) sold his private banking information to Venmo; and  
23 (d) monetized his private banking data by performing analytics on it and using it to develop  
24 value-added products for Plaid's customers. Mr. Sotelo did not and does not consent to these  
25 activities.

26 186. Mr. Sotelo has suffered actual and concrete injury as a result of Plaid's  
27 misconduct, including, *inter alia*, economic damages caused by the misappropriation of his  
28 sensitive financial and personal data, and harm to his dignitary rights and interests as a human

1 being related to unauthorized parties accessing, storing, selling, and using his most private  
2 financial information and intruding upon his private affairs and concerns. He is also at increased  
3 risk of identity theft and fraud and monitors his credit, bank, and other account statements on  
4 almost a daily basis for evidence of identity theft and fraud. He anticipates continuing to do so for  
5 the foreseeable future.

6 187. Mr. Sotelo's financial account at Bank of America was "linked" to and verified for  
7 use with the Venmo app. Mr. Sotelo has used Bank of America's password-protected interface  
8 with its servers and systems to receive communications about his financial account, including  
9 without limitation bank statements addressed to him and a listing of his recent account activity, as  
10 well as messages, notifications, and other transfers of information.

11 188. Plaintiff **Jeffrey Umali** signed up to use the Venmo app in or about 2015, and the  
12 Cash App app in or about 2016, via his mobile phone. When Mr. Umali established his accounts  
13 with Venmo and Cash App, he did so for the purpose, consistent with the services offered by  
14 Venmo and Cash App, of being able to send and receive payments to or from friends,  
15 acquaintances, and other consumers.

16 189. Mr. Umali also signed up to use the Coinbase app in or about 2017, via his mobile  
17 phone. When Mr. Umali established his account with Coinbase, he did so for the purpose,  
18 consistent with the services offered by Coinbase, of being able to buy and sell bitcoin.

19 190. To the extent Mr. Umali recalls specific details about the process of linking his  
20 bank account to his Venmo, Cash App, and Coinbase accounts so that he could send and receive  
21 money through the apps, those details are consistent with the discussion of Plaid's interface  
22 herein. Mr. Umali does not recall being prompted to read any privacy policy from Plaid during  
23 the process of logging into his bank account and does not recall having ever read any privacy  
24 policy from Plaid when he linked his bank account to each app.

25 191. At the times Mr. Umali established his accounts with Venmo, Cash App, and  
26 Coinbase, he was not aware of the existence or role of Plaid. When he was prompted in the  
27 Venmo, Cash App, and Coinbase apps to log into his bank account, he believed he was doing so  
28

1 through an official connection with his bank. He was unaware that he was providing his login  
2 credentials to Plaid.

3 192. When Mr. Umali was prompted in the Venmo, Cash App, and Coinbase apps to  
4 log into his bank account, he was not aware that Plaid: (a) would collect any of his banking  
5 information as part of that process; (b) would collect, receive, or store any of his banking  
6 information beyond that which was strictly necessary to effectuate transfer or receipt of payments  
7 from or to his bank account; (c) would collect, receive, or store any transaction-related banking  
8 information beyond the specific transactions he triggered using the Venmo, Cash App, and  
9 Coinbase apps; (d) would sell his banking data to Venmo, Cash App, and Coinbase; or (e) would  
10 use or monetize his banking data in any way. On the contrary, Mr. Umali reasonably expected  
11 that such conduct would not occur.

12 193. By logging into his bank account when prompted in the Venmo, Cash App, and  
13 Coinbase apps, Mr. Umali intended only to prompt his bank to provide Venmo, Cash App, and  
14 Coinbase, respectively, with a connection to his account for the limited purposes of withdrawing  
15 funds for transfers he triggered in the apps and depositing funds for transfers other app users  
16 made to him.

17 194. If Mr. Umali had learned what he now knows about the existence and role of Plaid,  
18 or the practices of Plaid in collecting, receiving, storing, selling, or using his banking data, he  
19 would not have connected his bank account in the Venmo, Cash App, and Coinbase apps the way  
20 he did.

21 195. Since the time Mr. Umali established his account with Cash App, he has used the  
22 app sparingly.

23 196. Mr. Umali is informed and believes that Plaid: (a) collected his private bank login  
24 credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed his private  
25 banking information and data; (c) sold his private banking information to Venmo, Cash App, and  
26 Coinbase; and (d) monetized his private banking data by performing analytics on it and using it to  
27 develop value-added products for Plaid's customers. Mr. Umali did not and does not consent to  
28 these activities.

1           197. Mr. Umali has suffered actual and concrete injury as a result of Plaid's  
2 misconduct, including, *inter alia*, economic damages caused by the misappropriation of his  
3 sensitive financial and personal data, and harm to his dignitary rights and interests as a human  
4 being related to unauthorized parties accessing, storing, selling, and using his most private  
5 financial information and intruding upon his private affairs and concerns. He is also at increased  
6 risk of identity theft and fraud and monitors his credit, bank, and other account statements on  
7 almost a daily basis for evidence of identity theft and fraud. He anticipates continuing to do so for  
8 the foreseeable future.

9           198. Mr. Umali's financial account at Chase Bank was "linked" to and verified for use  
10 with the Venmo, Cash App, and Coinbase apps. Mr. Umali has used Chase Bank's password-  
11 protected interface with its servers and systems to receive communications about his financial  
12 account, including without limitation bank statements addressed to him and a listing of his recent  
13 account activity, as well as messages, notifications, and other transfers of information.

14           199. Plaintiff **Nicholas Yeomelakis** signed up to use the Venmo app in or about March  
15 2014 via his mobile phone. When Mr. Yeomelakis established his account with Venmo, he did so  
16 for the purpose, consistent with the services offered by Venmo, of being able to send and receive  
17 payments to or from friends, acquaintances, and other consumers.

18           200. To the extent Mr. Yeomelakis recalls specific details about the process of linking  
19 his bank account to his Venmo account so that he could send and receive money through the app,  
20 those details are consistent with the discussion of Plaid's interface herein. Mr. Yeomelakis does  
21 not recall being prompted to read any privacy policy from Plaid during the process of logging into  
22 his bank account and does not recall having ever read any privacy policy from Plaid when he  
23 linked his bank account.

24           201. At the time Mr. Yeomelakis established his account with Venmo, he was not  
25 aware of the existence or role of Plaid. When he was prompted in the Venmo app to log into his  
26 bank account, he believed he was doing so through an official connection with his bank. He was  
27 unaware that he was providing his login credentials to Plaid.  
28

1           202. When Mr. Yeomelakis was prompted in the Venmo app to log into his bank  
2 account, he was not aware that Plaid: (a) would collect any of his banking information as part of  
3 that process; (b) would collect, receive, or store any of his banking information beyond that which  
4 was strictly necessary to effectuate transfer or receipt of payments from or to his bank account;  
5 (c) would collect, receive, or store any transaction-related banking information beyond the  
6 specific transactions he triggered using the Venmo app; (d) would sell his banking data to  
7 Venmo; or (e) would use or monetize his banking data in any way. On the contrary, Mr.  
8 Yeomelakis reasonably expected that such conduct would not occur.

9           203. By logging into his bank account when prompted in the Venmo app, Mr.  
10 Yeomelakis intended only to prompt his bank to provide Venmo with a connection to his account  
11 for the limited purposes of withdrawing funds for transfers he triggered in the Venmo account and  
12 depositing funds for transfers other Venmo users made to him.

13           204. If Mr. Yeomelakis had learned what he now knows about the existence and role of  
14 Plaid, or the practices of Plaid in collecting, receiving, storing, selling, or using his banking data,  
15 he would not have connected his bank account in the Venmo app the way he did.

16           205. Mr. Yeomelakis is informed and believes that Plaid: (a) collected his private bank  
17 login credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed his  
18 private banking information and data; (c) sold his private banking information to Venmo; and  
19 (d) monetized his private banking data by performing analytics on it and using it to develop  
20 value-added products for Plaid's customers. Mr. Yeomelakis did not and does not consent to  
21 these activities.

22           206. Mr. Yeomelakis has suffered actual and concrete injury as a result of Plaid's  
23 misconduct, including, *inter alia*, economic damages caused by the misappropriation of his  
24 sensitive financial and personal data, and harm to his dignitary rights and interests as a human  
25 being related to unauthorized parties accessing, storing, selling, and using his most private  
26 financial information and intruding upon his private affairs and concerns. He is also at increased  
27 risk of identity theft and fraud and regularly monitors his credit, bank, and other account  
28



1 statements for evidence of identity theft and fraud. He anticipates continuing to do so for the  
2 foreseeable future.

3 207. Mr. Yeomelakis's financial account at Bank of America was "linked" to and  
4 verified for use with the Venmo app. Mr. Yeomelakis has used Bank of America's password-  
5 protected interface with its servers and systems to receive communications about his financial  
6 account, including without limitation bank statements addressed to him and a listing of his recent  
7 account activity, as well as messages, notifications, and other transfers of information.

8 **B. Injuries from Invasions of Privacy and Dignitary Violations**

9 208. Plaintiffs and Class members suffered a massive invasion of privacy and intrusion  
10 upon their dignitary rights when Plaid, without their knowledge or consent, obtained access to  
11 their personal financial accounts and stripped out all available data, including without limitation:  
12 (a) their account numbers; (b) years of transactional data for every linked account (revealing how  
13 they prioritized expenses; what they spent money on; and where and when they spent it, including  
14 the name of the merchant and transaction amount as well as the address and geolocation where  
15 each transaction occurred); (c) account balances; (d) their detailed personal information including  
16 names, addresses, phone numbers, and emails; (e) detailed investment information, including  
17 current holdings, value and cost basis of investments, and investment transaction history;  
18 (f) information about annual salary and income sources (*i.e.*, employment information); (g)  
19 detailed information about liabilities, including payment histories, historical balances, and interest  
20 rates; and (h) bank account and other identifying information about their minor children.<sup>76</sup>  
21 Plaintiffs and Class members reasonably believed that this information was private and would not  
22 be accessible without their informed consent. Each time that Plaid gathered, used, sold,  
23 transmitted, and stored this incredibly sensitive and personal information, Plaid invaded  
24 Plaintiffs' and Class members' financial and other privacy rights and violated their dignitary  
25 interests.

26  
27  
28 <sup>76</sup> See <https://plaid.com/docs/>;  
<https://web.archive.org/web/20160319102824/https://plaid.com/docs/>.

1           209. In addition, Plaintiffs and Class members suffered invasions of privacy when Plaid  
2 collected, analyzed, sold, and used their medical-related personally identifiable information, in  
3 violation of requirements under HIPAA. Examples of such information are transactional data  
4 related to expenditures for doctors, hospitals, clinics and other health care facilities, as well as  
5 expenditures for prescription drugs and other treatments. Examples also include data connected  
6 with healthcare-related liabilities, such as medical payment plans or loans for elective surgeries.  
7 Plaintiffs and Class members reasonably believed that this information was private. Each time  
8 that Plaid gathered, used, sold, transmitted, and stored this information, Plaid invaded Plaintiffs'  
9 and Class members' right to privacy.

10           210. These invasions represent an egregious violation of established social norms.  
11 Plaid's conduct violates its acknowledged obligations under the existing regulatory scheme for  
12 financial institutions and defies common law privacy protections as well as standard practice in  
13 the financial industry. Consumers uniformly recognize the sensitivity of financial account  
14 information and reasonably expect adequate disclosures and protections, even in the context of  
15 sharing with financial applications with which, unlike Plaid, consumers *intentionally* interact to  
16 obtain "traditional banking services," including personal financial management and budgeting  
17 services.

18           211. The privacy, sensitivity, and appropriate safeguarding of confidential financial  
19 information are material to consumers. This materiality is reflected in the various statutes that  
20 enshrine these principles and the long history of the common law (put another way, privacy is  
21 material as a matter of law), as well as through numerous other sources.

22           212. For example, the materiality of maintaining financial privacy was confirmed in a  
23 2018 survey about fintech apps and financial data by The Clearing House ("TCH"), a banking  
24 association and payments company owned by the largest commercial banks. While Plaid was not  
25 addressed by the survey—unsurprisingly given consumers' general unawareness of it—and while  
26 many of the survey participants likely used apps for more involved purposes than the  
27 Participating Apps (which exist largely to facilitate payments), the relevant conclusions include:  
28

1 a. High levels of sensitivity about data access and privacy. Virtually all consumers  
2 (a full 99%) expressed at least some concern about data privacy and data sharing, and indeed  
3 more than two-thirds (67%) were very or extremely concerned.<sup>77</sup>

4 b. Low levels of consumer understanding. Notwithstanding this universal concern,  
5 “[b]etween 62% and 81% of financial app users are not aware that the apps may access a range  
6 of data types, from their email address to their bank account username and password. Between  
7 81% and 86% of users are not fully aware that the apps may take actions such as sell their data to  
8 third parties or retain access to information even when the app is deleted.”<sup>78</sup> In an interview  
9 regarding the survey results, a senior VP of The Clearing House explained that consumer  
10 confusion was likely related to the speed at which consumers sign up for apps and the “design of  
11 the apps themselves,” such as where “third-party apps” (*i.e.*, Plaid) “ask for your bank  
12 credentials while displaying your bank’s logo and colors.” He continued, “You might think ‘Oh,  
13 I’m actually connecting directly to a bank.’ They don’t necessarily realize that the bank actually  
14 has nothing to do with that.” In other words, low levels of consumer understanding flow directly  
15 from Plaid’s spoofing and other deceptive business practices.<sup>79</sup>

16 c. Consumers would like controls over third party access and use of data. A full 96%  
17 of respondents cared about how their data was accessed and, while some favored having their  
18 primary bank control who had access to their information, most wanted control and the right to  
19 provide explicit consent.<sup>80</sup>

20 213. Again, this survey did not even purport to address the facts where, as here, a  
21 company disguises itself as a trusted financial institution, and uses and profits from the

22 <sup>77</sup> See Aug. 2018 publication by The Clearing House: *Fintech Apps and Data Privacy: New*  
23 *Insights from Consumer Research*, [https://www.theclearinghouse.org/payment-](https://www.theclearinghouse.org/payment-systems/articles/2018/10/-/media/d025e3d1e5794a75a0144e835cd056b3.ashx)  
24 [systems/articles/2018/10/-/media/d025e3d1e5794a75a0144e835cd056b3.ashx](https://www.theclearinghouse.org/payment-systems/articles/2018/10/-/media/d025e3d1e5794a75a0144e835cd056b3.ashx); see also The  
25 Clearing House infographic, [https://www.theclearinghouse.org/payment-](https://www.theclearinghouse.org/payment-systems/articles/2018/10/-/link.aspx?_id=22B1B06FB2B143CAA2E9DE8634064E00&_z=z)  
[systems/articles/2018/10/-/link.aspx?\\_id=22B1B06FB2B143CAA2E9DE8634064E00&\\_z=z](https://www.theclearinghouse.org/payment-systems/articles/2018/10/-/link.aspx?_id=22B1B06FB2B143CAA2E9DE8634064E00&_z=z).

26 <sup>78</sup> *Id.*

27 <sup>79</sup> See Nov. 19, 2019 Bankrate article: *80% of Financial App Users Admit not Fully Realizing*  
28 *Their Banking Credentials are Shared: Survey*, [https://www.bankrate.com/banking/financial-](https://www.bankrate.com/banking/financial-apps-banking-data-privacy-survey/)  
[apps-banking-data-privacy-survey/](https://www.bankrate.com/banking/financial-apps-banking-data-privacy-survey/).

<sup>80</sup> See Aug. 2018 publication by The Clearing House: *Fintech Apps and Data Privacy: New*  
*Insights from Consumer Research*, [https://www.theclearinghouse.org/payment-](https://www.theclearinghouse.org/payment-systems/articles/2018/10/-/media/d025e3d1e5794a75a0144e835cd056b3.ashx)  
[systems/articles/2018/10/-/media/d025e3d1e5794a75a0144e835cd056b3.ashx](https://www.theclearinghouse.org/payment-systems/articles/2018/10/-/media/d025e3d1e5794a75a0144e835cd056b3.ashx), at 7.

information it acquires. The TCH survey defined “fintech apps” broadly to include “desktop or mobile financial applications that provide **traditional banking services**, including personal financial management services, budgeting/saving services, investment services, advisory services and/or lending services.”<sup>81</sup> The results of the survey would have revealed even more sensitivity to privacy and disclosure issues if the focus were on fintech apps, like the Participating Apps, that have the more limited function of enabling payments. The survey results thus strongly underscore the materiality of Plaid’s omissions and concealment concerning Plaintiffs’ and Class members’ financial privacy at issue here.

### C. Economic Damages

214. Plaintiffs and Class members also suffered significant economic damages, including: (a) the loss of valuable indemnification rights; (b) the diminished value of important data protection rights they possessed when their sensitive information was secured in the banking environment; (c) the loss of control over valuable property; and (d) the heightened risk of identity theft and fraud.

#### 1. Loss of Valuable Indemnification Rights

215. Plaintiffs and Class members suffered economic damages when Plaid deceptively acquired their bank login credentials and informed their financial institutions that they had provided Plaid with permission to gain access to all information available in their bank accounts; Plaid’s conduct destroyed valuable indemnity rights possessed by Plaintiffs and Class members.

216. These rights arise from Regulation E, codified at 12 C.F.R. § 1005, which provides a number of legal protections for consumers when their login credentials at financial institutions are used, unbeknownst to them, to conduct unauthorized electronic funds transfers. Among other protections, a consumer’s liability for an unauthorized transfer is typically limited to a maximum of either \$50 or \$500, depending upon how soon the bank was notified of the unauthorized transfer. 12 C.F.R. § 1005.6.

217. Regulation E defines an “[u]nauthorized electronic fund transfer” as “an electronic fund transfer from a consumer’s account initiated by a person other than the consumer without

---

<sup>81</sup> *Id.* (emphasis added).

1 actual authority to initiate the transfer and from which the consumer receives no benefit.” 12  
 2 C.F.R. § 1005.2(m).

3 218. Plaid’s conduct eliminates consumers’ rights under Regulation E because the  
 4 provision of login credentials may be construed as a grant of “authority” to conduct funds  
 5 transfers. Specifically, banks have taken the position that where a consumer provides login  
 6 credentials to a third party and an unauthorized transfer is then initiated by either the third party  
 7 or another outside source as a result of a breach of the third party, “the transfer would be  
 8 considered authorized by the bank because the client had furnished an access device (*i.e.* login  
 9 credentials) to the [third party], leaving the customer liable for such transfers.”<sup>82</sup>

10 219. The American Bankers Association has taken the position that banks are not liable  
 11 under Regulation E for unauthorized transactions made by data aggregators, such as Plaid, to  
 12 whom the consumer has provided login credentials. As a result, according to the Association,  
 13 “banks are not liable” for unauthorized transactions made via data aggregators like Plaid, and if  
 14 the aggregators are “unable or unwilling to reimburse the consumer, the consumer suffers the  
 15 loss.”<sup>83</sup> Chase’s CEO likewise stated that “[w]hen customers give out their bank passcode, they  
 16 may not realize that if a rogue employee at an aggregator uses this passcode to steal money from  
 17 the customer’s account, the customer, not the bank, is responsible for any loss.”<sup>84</sup>

18 220. As recognized by the American Bankers Association, when Plaid collected  
 19 Plaintiffs’ and Class members’ sensitive financial information, that information left the “secure  
 20 bank environment, where it is accorded longstanding legal protections, and [was] released into the  
 21 data services market where it is accorded no more special status than data created through a  
 22 consumer’s use of a social media platform.”<sup>85</sup>

23 <sup>82</sup> See Feb. 21, 2017 Response by Consumer Bankers Association to CFPB RFI,  
 24 <https://www.consumerbankers.com/sites/default/files/CFPB%20-%20Docket%20No%20-%202016-0048%20-%20RFI%20Consumer%20Access%20to%20Financial%20Records.pdf>.

25 <sup>83</sup> See Feb. 21, 2017 Response by American Bankers Association to CFPB RFI,  
 26 <https://buckleyfirm.com/sites/default/files/Buckley%20Sandler%20InfoBytes%20-%20American%20Bankers%20Association%202017.02.21%20Comment%20Letter%20to%20CFPB%27s%20RFI%20CFPB-2016-0048.pdf>.

27 <sup>84</sup> See Apr. 6, 2016 Letter from JPMorgan Chase to shareholders,  
 28 <https://www.jpmorganchase.com/corporate/annual-report/2015/>.

<sup>85</sup> See Feb. 21, 2017 Response by American Bankers Association to CFPB RFI,

221. Thus, when Plaid collects and uses consumers' bank login information and purports to have consumers' consent to Plaid's extraction and subsequent uses and sale of their data, Plaid removes valuable protections afforded to those consumers in the event of unauthorized transfers. Plaid has deprived those consumers of rights to be indemnified and reimbursed for the amount of such transfers over the limit (*e.g.*, a consumer's right to be indemnified for \$9,950 for an unauthorized \$10,000 transaction that was reported the next day).

222. In recognition of the severe impact of this loss of protection for consumers as a result of data aggregators' practices, in May 2018, three prominent aggregators submitted a new proposed framework (the "Soda framework") for the industry to follow in lieu of new government regulation. Included in the core principles of the Soda framework was the requirement that "[t]he entity responsible for a consumer's financial loss must make the consumer whole." As described in an *American Banker* article, the Soda framework "answers a long-held question on liability in saying the entity responsible for a consumer's financial loss must make that consumer whole. For loss occurring due to the actions of a data aggregator's clients, the aggregator would be responsible to "reasonably establish that [its clients] have capacity, through capital, insurance, or any other means, to make whole any consumers who suffer a financial loss as a result of a breach."<sup>86</sup>

223. Plaid, however, ensures that consumers' loss of valuable indemnification rights is complete. In stark contrast to the guidelines in the Soda framework, Plaid makes no offer to indemnify users of the Participating Apps for fraudulent activity on their financial accounts or other fraud perpetrated with use of their login credentials.

224. As a result, even while Plaid has robbed consumers of the valuable protections afforded them in the event of unauthorized transfers using their bank information, it

---

<https://buckleyfirm.com/sites/default/files/Buckley%20Sandler%20InfoBytes%20-%20American%20Bankers%20Association%202017.02.21%20Comment%20Letter%20to%20CFPB%27s%20RFI%20CFPB-2016-0048.pdf>.

<sup>86</sup> See May 10, 2018 *American Banker* article, *Who's on the hook for a hack? Aggregators team up on answer*, <https://www.americanbanker.com/news/envestnet-yodlee-quovo-byallaccounts-unveil-data-sharing-framework>.

1 simultaneously has attempted to shield itself from any liability for unauthorized transfers that  
2 occur as a result of its activities.

### 3 **2. Diminished Value of Rights to Protection of Data**

4 225. Plaintiffs and Class members suffered additional economic damages through  
5 diminished value of their rights to protection of their banking data.

6 226. Without their knowledge or consent, Plaid: (a) took their most sensitive financial  
7 information out of their banks' trusted, secure environment; (b) sold it to the Participating Apps  
8 without adequate controls over what such apps would do with it; and (c) stored the information  
9 elsewhere for its own purposes, including without limitation for the purposes of "enriching" and  
10 analyzing it.

11 227. As the American Bankers Association has recognized, when data aggregators such  
12 as Plaid move data out of the secure banking environment, they deprive consumers of valuable  
13 protections afforded by law when the data resides in that environment.<sup>87</sup>

### 14 **3. Loss of Control Over Valuable Property**

15 228. Plaintiffs and Class members suffered loss of use and control to Plaid of their own  
16 sensitive financial information, property which has value to them.

17 229. There can be no question that Plaintiffs' and Class members' sensitive financial  
18 information is property that has value. As an initial matter, that information obviously has  
19 significant *present financial value* because (a) Plaid has built a very successful business,  
20 generating tens of millions of dollars annually, off of selling that information to companies like  
21 the Participating Apps; and (b) Visa has agreed to pay \$5.3 billion for Plaid, based mainly upon  
22 the value of that financial information.

23 230. For the same reasons, Plaid has established that a market exists for Plaintiffs' and  
24 Class members' sensitive financial information. That financial information has significant *future*  
25 *financial value* to Plaid as well, which is evident given the company's plans to pivot and focus on  
26

27 <sup>87</sup> See Feb. 21, 2017 Response by American Bankers Association to CFPB RFI,  
28 <https://buckleyfirm.com/sites/default/files/Buckley%20Sandler%20InfoBytes%20-%20American%20Bankers%20Association%202017.02.21%20Comment%20Letter%20to%20CFPB%27s%20RFI%20CFPB-2016-0048.pdf>.



monetizing that information through analytics and value-added services it builds using that information. It also has significant *competitive value* to Plaid, providing the company with a moat to protect its position against would-be competitors.

231. Plaintiffs and Class members suffered harm when Plaid took their property, sold it, and put it to use for present and future monetization in other forms, for its own enrichment.

#### 4. **Increased Risk of Identity Theft and Fraud**

232. In addition to removing valuable existing protections, Plaid's actions in removing Plaintiffs' and Class members' sensitive banking data from the secure banking environment also create huge additional risks for Plaintiffs:

[T]he sheer volume and value of the aggregated data make data aggregators a priority target for criminals, including identity thieves. . . . Through a single source, the criminal may gain access to the consumer's checking and savings accounts, retirement accounts, certificates of deposits, credit cards, brokerage accounts, and insurance products. . . . This rich reward for a single hack, either of an aggregated database of personally identifiable information or of a single consumer's multiple accounts, makes data aggregators an attractive target for criminals. They obtain the key not to just a single room, but the key ring with keys to all the rooms.<sup>88</sup>

233. Plaid knowingly magnified this risk by creating a single point of failure whereby all consumers' bank login credentials, personal information, and banking data could be accessed through a single attack.

234. These risks have created tangible, economic injury to Plaintiffs and Class members. One such risk is that someone at Plaid, Venmo, or one of their partner companies, vendors or contractors (*e.g.*, an outside software developer) will use Plaintiffs' and Class members' banking information to conduct unauthorized transactions, causing direct financial loss to them. Other risks include identity theft and fraud using Plaintiffs' and Class members' private banking information and data, which may result in long-term injuries related to compromised accounts, damaged credit ratings, inability to obtain credit, fraudulent tax filings, dissemination of

<sup>88</sup> See Feb. 21, 2017 Response by American Bankers Association to CFPB RFI, <https://buckleyfirm.com/sites/default/files/Buckley%20Sandler%20InfoBytes%20-%20American%20Bankers%20Association%202017.02.21%20Comment%20Letter%20to%20CFPB%27s%20RFI%20CFPB-2016-0048.pdf>.



1 inaccurate or fraudulent medical information, and loss of employment opportunities. The integrity  
 2 of Plaintiffs' and Class members' bank accounts and the banking information and data therein has  
 3 been permanently diminished, and now they face an expanded and imminent risk of economic  
 4 harm from unauthorized transfers, identity theft, and fraud.

5 235. That Plaintiffs and Class members may not yet be aware that harm has occurred  
 6 increases rather than diminishes their risk because they cannot take specific action to prevent  
 7 harm. In addition, Plaintiffs and Class members face increased risk of predatory conduct by those  
 8 who obtain access to their personal information and data without their knowledge.

## 9 **VII. CHOICE OF LAW**

10 236. California's substantive laws may be constitutionally applied to the claims of  
 11 Plaintiffs and the Nationwide Class members under the Due Process Clause, 14th Amend., § 1,  
 12 and the Full Faith and Credit Clause, art. IV., § 1, of the U.S. Constitution.

13 237. California has a significant contact, or significant aggregation of contacts, to the  
 14 claims asserted by each Plaintiff, thereby creating state interests that ensure that the choice of  
 15 California state law to the common-law claims is not arbitrary or unfair. Plaid's headquarters and  
 16 principal place of business are in California. Plaid conducts substantial business in California, and  
 17 upon information and belief the scheme alleged in this Complaint originated and was  
 18 implemented in California. Class members' data is pulled, stored, and aggregated by Plaid in  
 19 California. California has a strong interest in regulating Plaid's conduct under its laws.

20 238. The application of California law to the proposed Nationwide Class members  
 21 (defined below) is also appropriate under California's choice of law rules, namely, the  
 22 governmental interest test California uses for choice-of-law questions. California's interest would  
 23 be the most impaired if its laws were not applied.

## 24 **VIII. TOLLING, CONCEALMENT, AND ESTOPPEL**

25 239. The statutes of limitation applicable to Plaintiffs' claims are tolled as a result of  
 26 Plaid's knowing and active concealment of its conduct alleged herein.

27 240. Among other things, Plaid made misleading statements in the Plaid software  
 28 incorporated in fintech apps and made misleading public statements (including in publications

and to various government agencies and regulators), while intentionally hiding its true actions and knowingly permitting the fintech apps to make statements that were misleading and concealed the true nature of Plaid's conduct and operation.

241. Moreover, Plaintiffs were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their own part.

242. Furthermore, under the circumstances Plaid was under a duty to disclose the true character, quality, and nature of its activities to Plaintiffs. Plaid therefore is estopped from relying on any statute of limitations.

243. All applicable statutes of limitation also have been tolled by operation of the discovery rule. Specifically, Plaintiffs and other Class members could not have learned through the exercise of reasonable diligence of Plaid's conduct as alleged herein.

244. Plaid's fraudulent concealment and omissions are common to all Class members.

#### **IX. CLASS ACTION ALLEGATIONS**

245. Plaintiffs incorporate by reference all the foregoing allegations.

246. Plaintiffs bring this action on behalf of themselves and all others similarly situated pursuant to Rule 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure.

247. Plaintiffs seek to represent the following Class:

**Nationwide Class:** All natural persons in the United States whose accounts at a financial institution were accessed by Plaid using login credentials obtained through Plaid's software incorporated in a mobile or web-based fintech app that enables payments (including ACH payments) or other money transfers, including without limitation users of Venmo, Square's Cash App, Coinbase, and Stripe, from January 1, 2013 to the present.

248. In addition, Plaintiffs James Cottle, David Evans, Logan Mitchell, Frederick Schoeneman, Gabriel Sotelo, and Jeffrey Umali seek to represent the following Class:

**California Class:** All natural persons in California whose accounts at a financial institution were accessed by Plaid using login credentials obtained through Plaid's software incorporated in a mobile or web-based fintech app that enables payments (including ACH payments) or other money transfers, including without limitation users of Venmo, Square's Cash App, Coinbase, and Stripe, from January 1, 2013 to the present.

249. Excluded from the Classes are Plaid, its current employees, co-conspirators, officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries or affiliated companies; the undersigned counsel for Plaintiffs and their employees; and the Judge and court staff to whom this case is assigned.

250. Plaintiffs expressly reserve the right to modify or amend the definition of the proposed Classes to conform to proof or otherwise, including to bring state-law classes for consumer protection or common-law claims should the Court hold that state law claims alleged herein may not be pursued on behalf of the Nationwide Class.

251. The Classes and their counsel satisfy the prerequisites of Federal Rule of Civil Procedure 23(a) and 23(g) and the requirements of Rule 23(b)(3).

252. Numerosity and Ascertainability: Plaintiffs do not know the exact size of the Classes or the identities of the Class members. Such information is known to Plaid. At minimum, each Class has thousands or millions of members. Reports indicate that Plaid has accessed approximately 200 million United States financial accounts. Venmo had over 52 million active accounts at the end of 2019.<sup>89</sup> Coinbase reportedly has more than 30 million users.<sup>90</sup> Square's Cash App reportedly has more than 24 million monthly active users.<sup>91</sup> Thus, the number of members in each Class is so numerous that joinder of all Class members is impracticable. The names, addresses, and phone numbers of Class members are identifiable through documents maintained by Plaid, and also available from the records of third parties such as Class members' financial institutions and the Participating Apps.

253. Commonality and Predominance: The action involves numerous common questions of law and fact that predominate over any question solely affecting individual Class members. These common questions for Class members' claims include, but are not limited to, the following:

- (1) Whether Plaid omitted or concealed material facts from Plaintiffs

<sup>89</sup> See <https://investor.paypal-corp.com/static-files/0b7b0dda-a4ee-4763-9eee-76c01be0622c>.

<sup>90</sup> See <https://www.coinbase.com/about>.

<sup>91</sup> See <https://www.businessinsider.com/squares-cash-app-reached-24-million-users-and-monetization-surge-2020-2>.

and Class members that it had a duty to disclose;

- (2) Whether Plaid gave effective notice of its privacy policy under an objectively reasonable consumer standard;
- (3) Whether Plaid's privacy policy discloses Plaid's conduct;
- (4) Whether Plaid obtained consent to obtain, store, and use Plaintiffs' and Class members' banking credentials and/or private financial information;
- (5) Whether Plaid's acts and practices complained of herein amount to egregious breaches of social norms under California law (as applied nationwide), or alternatively under each of the laws where Plaintiffs reside;
- (6) Whether Plaid's conduct described herein violates Plaintiffs' and Class members' interest in precluding the dissemination or misuse of sensitive, confidential information ("informational privacy");
- (7) Whether Plaid's conduct described herein violates Plaintiffs' and Class members' interest in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference ("autonomy privacy");
- (8) Whether the computer systems operated by Plaintiffs' and Class members' financial institutions are "protected computers" or "computers of financial institutions" under the CFAA;
- (9) Whether Plaid intentionally accessed protected computer systems in violation of the CFAA;
- (10) Whether Plaid's conduct violated the Stored Communications Act, 18 U.S.C. § 2701, *et seq.*;
- (11) Whether Plaid's conduct violated the California Constitution;
- (12) Whether Plaid, through its Managed OAuth process, induced California Class members to provide "identifying information"

1 within the meaning of the California Anti-Phishing Act by  
2 representing itself to be a business without the authority or  
3 approval of the business;

4 (13) Whether Plaintiffs and Class members are “adversely affected”  
5 within the meaning of the California Anti-Phishing Act by the  
6 collection of their financial institution login credentials and  
7 identifying information by Plaid or by Plaid’s subsequent use and  
8 sale of such information;

9 (14) Whether Plaid’s conduct constitutes an unlawful, unfair, or  
10 deceptive business practice under Cal. Bus. & Prof. Code § 17200,  
11 *et seq.* or, alternatively, under the consumer protection and/or  
12 UDAP statutes or the laws where Plaintiffs reside;

13 (15) Whether Plaintiffs and Class members are entitled to compensation  
14 resulting from the loss caused by Plaid of a right to indemnity by  
15 their financial institutions in the event of fraudulent conduct on  
16 their accounts, the heightened risk of identity theft and fraud  
17 caused by Plaid’s transfer of their identifying information from  
18 secure financial institutions to itself and to other parties, or  
19 otherwise;

20 (16) Whether any profits or other value obtained by Plaid through  
21 analysis, enrichment, and other use of information from Plaintiffs’  
22 and Class members’ financial accounts were unjustly obtained by  
23 Plaid and should be disgorged;

24 (17) Whether Plaintiffs and Class members are entitled to equitable  
25 compensation resulting from Plaid’s enrichment through its  
26 acquisition and use of Plaintiffs’ data and other conduct alleged  
27 herein; and

28 (18) Whether declaratory relief and an injunction should be granted.

1           254. Plaid engaged in a common course of conduct giving rise to the legal rights sought  
2 to be enforced by this action. Furthermore, similar or identical questions of statutory and common  
3 law, as well as similar or identical injuries, are involved. Individual questions, if any, pale in  
4 comparison to the numerous common questions that predominate in this action.

5           255. Typicality: Plaintiffs' claims are typical of the other Class members' claims  
6 because all Class members were comparably injured through Plaid's substantially uniform  
7 misconduct as described above. The Plaintiffs representing the Classes are advancing the same  
8 claims and legal theories on behalf of themselves and all other members of the Classes that they  
9 represent, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and  
10 Class members arise from the same operative facts and are based upon the same legal theories.

11           256. Adequacy: Plaintiffs are adequate Class representatives because their interests do  
12 not conflict with the interests of the other members of the Class they seek to represent; Plaintiffs  
13 have retained counsel competent and experienced in complex class action litigation, privacy law,  
14 and consumer fraud; and Plaintiffs intend to prosecute this action vigorously. The interests of the  
15 Classes will be fairly and adequately protected by Plaintiffs and their counsel.

16           257. Superiority: A class action is superior to any other available means for the fair and  
17 efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered  
18 in the management of this class action. The damages and other harm suffered by Plaintiffs and  
19 Class members are relatively small compared to the burden and expense that would be required to  
20 individually litigate their claims against Plaid, so it would be virtually impossible for Class  
21 members individually to seek redress for Plaid's wrongful conduct. Even if Class members could  
22 afford individual litigation, the court system could not. Individualized litigation creates a potential  
23 for inconsistent or contradictory judgments, and increases the delay and expense to all parties and  
24 the court system. By contrast, the class action device presents far fewer management difficulties,  
25 and provides the benefits of single adjudication, economy of scale, and comprehensive  
26 supervision by a single court.

27           258. Class certification under Rule 23(b)(2) is also warranted for purposes of injunctive  
28 and declaratory relief because Plaid has acted or refused to act on grounds generally applicable to

the Classes, so that final injunctive and declaratory relief are appropriate with respect to the Classes as a whole.

## **X. CLAIMS FOR RELIEF**

### **FIRST CAUSE OF ACTION**

#### **Invasion of Privacy—Intrusion into Private Affairs**

259. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein. These include the choice of law discussion. Specifically, California law on intrusion upon seclusion is applicable nationwide because there is no conflict of law between the law in California and in states that have expressly or, via jurisprudence, impliedly adopted the Restatement (Second) of Torts, § 652B or its constituent elements. Alternatively, no state has a greater interest than California in applying its laws.

260. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class (referred to in this claim as “the Class”).

261. Plaintiffs and Class members have a reasonable expectation of privacy in the personal information and banking data maintained at their banks. The reasonableness of this expectation is reflected in longstanding custom and practice, security measures intended to prevent unauthorized access to banking account information, state, federal, and international laws protecting a right to financial privacy, and the privacy policies and other assurances of protection by applications that use Plaid discussed herein, among other indicia. Plaintiffs and Class members reasonably expected that their login credentials, account numbers, balances, transaction history, and other information was private and secure within the banks at which they maintain accounts. They reasonably expected that their information and data (a) would be protected and secured against access by unauthorized parties; (b) would not be obtained by unauthorized parties; (c) would not be transmitted or stored outside of the secure bank environment; and (d) would not be sold or used without their knowledge or permission.

262. Plaid intentionally intruded upon Plaintiffs’ and Class members’ private affairs and concerns by improperly accessing, downloading, transferring, selling, storing and using their private banking information and data.

1           263. The manner in which Plaid obtained access to Plaintiffs' and Class members'  
2 banking login credentials, account numbers, balances, transaction history, and other information  
3 stored by their banks was highly offensive to Plaintiffs and would be highly offensive to a  
4 reasonable person. Each of (a) obtaining login credentials through covert means including by  
5 falsely suggesting, through use of design, overt and implied statements, and context, that  
6 consumers were communicating directly with their banks when they entered login credentials;  
7 (b) retaining login credentials for purposes other than verifying information about a consumer's  
8 bank account that was required for use of the relevant payment application; (c) using the illicitly-  
9 obtained login credentials to access historical banking information not required for use of the  
10 relevant payment application; (d) retaining, analyzing, and profiting from such information;  
11 (e) using the illicitly-obtained login credentials to access banking information after the date on  
12 which such credentials were initially provided; (f) retaining, analyzing, and profiting from such  
13 information; and (g) failing to disclose such conduct, constitute egregious violations of social  
14 norms.

15           264. Plaid's intrusions upon Plaintiffs' and Class members' private affairs and concerns  
16 would be highly offensive to a reasonable person, especially considering (a) the highly sensitive  
17 and personal nature of Plaintiffs' and Class members' banking information and data; (b) the  
18 extensive scope of data obtained by Plaid, including years of historical transactional data;  
19 (c) Plaid's intent to profit from Plaintiffs' and Class members' data by selling it outright and  
20 using it to develop further products and services; (d) Plaid's use of subterfuge to intrude into  
21 Plaintiffs' and Class members' banks' secure environments for the purpose of collecting their  
22 data; (e) the surreptitious and unseen nature of Plaid's data collection with respect to consumers,  
23 and (f) Plaid's failure to obtain consumers' consent to its conduct. Plaid's intrusions were  
24 substantial, and constituted an egregious breach of social norms.

25           265. Plaintiffs and Class members did not consent to Plaid's intrusions upon their  
26 private affairs and concerns.

27           266. Plaid's conduct described herein violates Plaintiffs' and Class members' interests  
28 in precluding the dissemination or misuse of sensitive and confidential information (*i.e.*, their



informational privacy rights), including without limitation the privacy of information about their income, generosity, charitable giving, retirement contributions, healthcare costs, healthcare treatment, shopping habits, dining habits, entertainment habits, saving and spending habits, credit repayment habits, locations, identity information including contact data, familial information, and other information available to their financial institutions, as well as the terms of any loans and other financial affairs.

267. Plaid's conduct described herein violates Plaintiffs' and Class members' interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference (*i.e.*, their autonomy privacy rights) because, without limitation, Plaid accesses the information described in the preceding paragraph multiple times per day, at a minimum every 4-6 hours, and analyzes the private information for its own undisclosed purposes including, *inter alia*, to generate invasive profiles of Plaintiffs' and Class members' incomes, debts, relationships, and personal lives.

268. Plaintiffs and Class members suffered actual and concrete injury as a result of Plaid's intrusions upon their private affairs and concerns. Plaintiffs and Class members are entitled to appropriate relief, including damages to compensate Plaintiffs and Class members for the harm to their privacy interests, loss of valuable rights and protections, heightened risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Plaid's invasions, as well as disgorgement of profits made by Plaid as a result of its intrusions upon Plaintiffs' and Class members' private affairs and concerns.

269. Plaintiffs and Class members also seek punitive damages because Plaid's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights. Punitive damages are warranted to deter Plaid from engaging in future misconduct.

## **SECOND CAUSE OF ACTION**

### **Violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030**

270. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

271. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class (referred to in this claim as “the Class”).

272. The CFAA prohibits unauthorized access to computers and the private financial data stored on those computers, as well as trafficking in password information for computers. Through its actions described herein, Plaid has committed multiple violations of the CFAA.

**A. Violations of 18 U.S.C. § 1030(a)(2)**

273. Plaid intentionally accessed a computer under 18 U.S.C. §§ 1030(a)(2) & 1030(e)(1) by intentionally accessing Plaintiffs’ and Class members’ personal financial accounts, and specifically the financial institutions’ computer systems, data storage facilities, or communications facilities.

274. Plaintiffs’ and Class members’ banks’ computer systems constitute both protected computers and computers of financial institutions under 18 U.S.C. §§ 1030(a)(2)(C) & 1030(e)(2)(A)-(B) because (i) they were exclusively for the use of a financial institution, (ii) they were used by a financial institution, and Plaid’s conduct affected the banks’ use of their systems, and (iii) they were used in or affected interstate or foreign commerce or communication.

275. Plaid violated 18 U.S.C. § 1030(a)(2)(A) when it intentionally accessed Plaintiffs’ and Class members’ banks’ computer systems without authorization, and thereby obtained information contained in a financial record of a financial institution, including all of the private data Plaid collected from Plaintiffs’ and Class members’ banking records. Plaintiffs and Class members did not grant express or implied authority for Plaid to access their banks’ computer systems.

276. Alternatively, Plaid violated 18 U.S.C. § 1030(a)(2)(A) when it intentionally accessed Plaintiffs’ and Class members’ banks’ computer systems and such access exceeded authorization, and thereby obtained information contained in a financial record of a financial institution. Plaintiffs and Class members did not grant express or implied authority for Plaid to access any data in their banks’ computer systems beyond that which was strictly necessary to facilitate transactions Plaintiffs and Class members conducted in the Participating Apps. Plaid exceeded authorized access under 18 U.S.C. § 1030(e)(6) by using its access to the banks’

1 computer systems to obtain information it was not entitled to obtain, in the form of data that was  
 2 not strictly necessary to facilitate Participating App transactions, including Plaintiffs' and Class  
 3 members' detailed banking transaction histories.

4 277. Plaid violated 18 U.S.C. § 1030(a)(2)(C) when it intentionally accessed Plaintiffs'  
 5 and Class members' banks' computer systems without authorization, and thereby obtained both  
 6 information in a financial record of a financial institution and information from a protected  
 7 computer, including all of the private data Plaid collected from Plaintiffs' and Class members'  
 8 banking records. Plaintiffs and Class members did not grant express or implied authority for Plaid  
 9 to access their banks' computer systems.

10 278. Alternatively, Plaid violated 18 U.S.C. § 1030(a)(2)(C) when it intentionally  
 11 accessed Plaintiffs' and Class members' banks' computer systems and such access exceeded  
 12 authorization, and thereby obtained both information in a financial record of a financial institution  
 13 and information from a protected computer. Plaintiffs and Class members did not grant express or  
 14 implied authority for Plaid to access any data in their banks' computer systems beyond that which  
 15 was strictly necessary to facilitate transactions Plaintiffs conducted in the Participating Apps.  
 16 Plaid exceeded authorized access under 18 U.S.C. § 1030(e)(6) by using its access to the banks'  
 17 computer systems to obtain information it was not entitled to obtain, in the form of data that was  
 18 not strictly necessary to facilitate Participating App transactions, including Plaintiffs' and Class  
 19 members' detailed banking transaction histories.

20 **B. Violations of 18 U.S.C. § 1030(a)(4)**

21 279. Plaid knowingly accessed a protected computer under 18 U.S.C. §§ 1030(a)(4) &  
 22 1030(e)(1)-(2) by knowingly accessing Plaintiffs' and Class members' banks' computer systems,  
 23 data storage facilities, or communications facilities.

24 280. Plaid acted with intent to defraud in accessing a protected computer under 18  
 25 U.S.C. §§ 1030(a)(4) & 1030(e)(1)-(2) by accessing Plaintiffs' and Class members' banks'  
 26 computer systems, data storage facilities, or communications facilities with the intent to collect  
 27 banking data to which it was not entitled and which it intended to sell and use without authority.  
 28

1           281. Plaid violated 18 U.S.C. § 1030(a)(4) when it intentionally accessed Plaintiffs’  
 2 banks’ computer systems without authorization, and thereby furthered its intended fraud and  
 3 obtained a thing of value, including all of the private data Plaid collected from Plaintiffs’ and  
 4 Class members’ banking records, as well as the use of the banks’ computer system. Plaintiffs and  
 5 Class members did not grant express or implied authority for Plaid to access their banks’  
 6 computer systems.

7           282. Alternatively, Plaid violated 18 U.S.C. § 1030(a)(4) when it intentionally accessed  
 8 Plaintiffs’ and Class members’ banks’ computer systems and such access exceeded authorization,  
 9 and thereby furthered its intended fraud and obtained a thing of value, including all of the private  
 10 data Plaid collected from Plaintiffs’ and Class members’ banking records, as well as the use of the  
 11 banks’ computer systems. Plaintiffs and Class members did not grant express or implied authority  
 12 for Plaid to access any data in their banks’ computer systems beyond that which was strictly  
 13 necessary to facilitate transactions Plaintiffs and Class members conducted in the Participating  
 14 Apps. Plaid exceeded authorized access under 18 U.S.C. § 1030(e)(6) by using its access to the  
 15 banks’ computer systems to obtain information it was not entitled to obtain, in the form of data  
 16 that was not strictly necessary to facilitate Participating App transactions, including Plaintiffs’  
 17 and Class members’ detailed banking transaction histories.

18           **C. Violations of 18 U.S.C. § 1030(a)(5)(A)**

19           283. Plaid knowingly caused the transmission of a program, information, code, or  
 20 command under 18 U.S.C. § 1030(a)(5)(A) by (1) knowingly transmitting Plaintiffs’ and Class  
 21 members’ bank login information to access their banks’ computer systems, data storage facilities,  
 22 or communications facilities; and (2) knowingly transmitting its software to the Participating  
 23 Apps for incorporation into their apps so that Plaid could collect Plaintiffs’ and Class members’  
 24 bank login information.

25           284. Plaid violated 18 U.S.C. § 1030(a)(5)(A) when it knowingly caused the  
 26 transmission of a program, information, code, or command, and as a result, intentionally caused  
 27 damage without authorization to the banks’ computer systems and Plaintiffs’ and Class members’  
 28

1 data contained therein, as well as to Plaintiffs' and Class members' smartphones and their data  
2 contained therein.

3 285. Plaid caused Plaintiffs and Class members damage under 18 U.S.C.  
4 §§ 1030(a)(5)(A) and 1030(e)(8), including in the following ways:

5 a. Plaid removed Plaintiffs' and Class members' banking data from the secure  
6 banking environment and placed it in an environment where it was subject to increased risk of  
7 loss or theft, including by selling or transferring it to the Participating Apps and by storing it for  
8 its own use. Plaid thereby destroyed the valuable indemnification rights Plaintiffs and Class  
9 members had against loss when that data was in the bank environment. Plaid also thereby  
10 removed valuable additional protections (including regulatory protections) Plaintiffs' and Class  
11 members' data had when that data was in the bank environment. As a result, the integrity of  
12 Plaintiffs' and Class members' data has been irreparably impaired.

13 b. Plaid used its software to obtain an open connection to Plaintiffs' and Class  
14 members' bank accounts so that it could control access to, and take information from, Plaintiffs'  
15 banks' computer systems. Plaid thereby impaired the integrity of both the banks' computer  
16 systems and Plaintiffs' and Class members' data contained therein.

17 c. Plaid impaired the integrity of Plaintiffs' and Class members' smartphones by  
18 installing software within the Participating Apps that captured their sensitive bank login data for  
19 use in logging into Plaintiffs' and Class members' bank accounts. Plaid thereby impaired the  
20 integrity of both Plaintiffs' and Class members' smartphones and their data contained therein.

21 d. Plaid accessed Plaintiffs' and Class members' bank' computer systems, copied  
22 their banking data, sold it to the Participating Apps, and used it for its own purposes. Plaid  
23 thereby impaired the integrity of both the banks' computer systems and Plaintiffs' and Class  
24 members' data contained therein.

25 **D. Violations of 18 U.S.C. § 1030(a)(5)(B)**

26 286. Plaid intentionally accessed a protected computer under 18 U.S.C.  
27 §§ 1030(a)(5)(B) & 1030(e)(1)-(2) by (1) intentionally accessing Plaintiff's and Class members'  
28 banks' computer systems, data storage facilities, or communications facilities; and

1 (2) intentionally accessing Plaintiffs' and Class members' smartphones by incorporating its  
2 software into the Participating Apps so that Plaid could collect Plaintiffs' and Class members'  
3 bank login information.

4 287. Plaid violated 18 U.S.C. § 1030(a)(5)(B) when it intentionally accessed a protected  
5 computer without authorization, and thereby at least recklessly caused damage to the banks'  
6 computer systems and Plaintiffs' and Class members' data contained therein, as well as to  
7 Plaintiffs' and Class members' smartphones and their data contained therein. Plaintiffs and Class  
8 members did not grant express or implied authority for Plaid to access either their banks'  
9 computer systems or their smartphones.

10 288. Plaid caused Plaintiffs and Class members damage under 18 U.S.C.  
11 §§ 1030(a)(5)(A) and 1030(e)(8), including in the following ways:

12 a. Plaid removed Plaintiffs' and Class members' banking data from the secure  
13 banking environment and placed it in an environment where it was subject to increased risk of  
14 loss or theft, including by selling or transferring it to the Participating Apps and by storing it for  
15 its own use. Plaid thereby destroyed the valuable indemnification rights Plaintiffs and Class  
16 members had against loss when that data was in the bank environment. Plaid also thereby  
17 removed valuable additional protections (including regulatory protections) Plaintiffs' and Class  
18 members' data had when that data was in the bank environment. As a result, the integrity of  
19 Plaintiffs' and Class members' data has been irreparably impaired.

20 b. Plaid used its software to obtain an open connection to Plaintiffs' and Class  
21 members' bank accounts so that it could control access to, and steal information from, Plaintiffs'  
22 and Class members' banks' computer systems. Plaid thereby impaired the integrity of both the  
23 banks' computer systems and Plaintiffs' and Class members' data contained therein.

24 c. Plaid impaired the integrity of Plaintiffs' and Class members' smartphones by  
25 installing software within the Participating Apps that captured their sensitive bank login data for  
26 use in logging into Plaintiffs' and Class members' bank accounts. Plaid thereby impaired the  
27 integrity of both Plaintiffs' and Class members' smartphones and their data contained therein.  
28

d. Plaid accessed Plaintiffs' and Class members' banks' computer systems, copied Plaintiffs' and Class members' banking data, sold it to the Participating Apps, and used it for its own purposes. Plaid thereby impaired the integrity of both the banks' computer systems and Plaintiffs' and Class members' data contained therein.

**E. Violations of 18 U.S.C. § 1030(a)(5)(C)**

289. Plaid intentionally accessed a protected computer under 18 U.S.C. §§ 1030(a)(5)(C) & 1030(e)(1)-(2) by (1) intentionally accessing Plaintiffs' and Class members' banks' computer systems, data storage facilities, or communications facilities; and (2) intentionally accessing Plaintiffs' and Class members' smartphones by incorporating its software into the Participating Apps so that Plaid could collect Plaintiffs' and Class members' bank login information.

290. Plaid violated 18 U.S.C. § 1030(a)(5)(C) when it intentionally accessed a protected computer without authorization, and thereby caused both damage and loss to the banks' computer systems and Plaintiffs' and Class members' data contained therein, as well as to Plaintiffs' and Class members' smartphones and their data contained therein. Plaintiffs and Class members did not grant express or implied authority for Plaid to access either their banks' computer systems or their smartphones.

291. Plaid caused Plaintiffs and Class members damage under 18 U.S.C. §§ 1030(a)(5)(A) and 1030(e)(8), including in the following ways:

a. Plaid removed Plaintiffs' and Class members' banking data from the secure banking environment and placed it in an environment where it was subject to increased risk of loss or theft, including by selling or transferring it to the Participating Apps and by storing it for its own use. Plaid thereby destroyed the valuable indemnification rights Plaintiffs and Class members had against loss when that data was in the bank environment. Plaid also thereby removed valuable additional protections (including regulatory protections) Plaintiffs' and Class members' data had when that data was in the bank environment. As a result, the integrity of Plaintiffs' and Class members' data has been irreparably impaired.



b. Plaid used its software to obtain an open connection to Plaintiffs' and Class members' bank accounts so that it could control access to, and steal information from, Plaintiffs' and Class members' banks' computer systems. Plaid thereby impaired the integrity of both the banks' computer systems and Plaintiffs' and Class members' data contained therein.

c. Plaid impaired the integrity of Plaintiffs' and Class members' smartphones by installing software within the Participating Apps that captured their sensitive bank login data for use in logging into Plaintiffs' and Class members' bank accounts. Plaid thereby impaired the integrity of both Plaintiffs' and Class members' smartphones and their data contained therein.

d. Plaid accessed Plaintiffs' and Class members' bank' computer systems, copied Plaintiffs' and Class members' banking data, sold it to the Participating Apps, and used it for its own purposes. Plaid thereby impaired the integrity of both the banks' computer systems and Plaintiffs' and Class members' data contained therein

292. Plaid caused Plaintiffs and Class members loss under 18 U.S.C. §§ 1030(a)(5)(A) and 1030(e)(11), including in the following ways:

a. Plaid removed Plaintiffs' and Class members' banking data from the secure banking environment, selling or transferring it to the Participating Apps and storing it for its own use. Plaid thereby (1) destroyed the valuable indemnification rights Plaintiffs and Class members had against loss when that data was in the bank environment; and (2) removed valuable additional protections (including regulatory protections) Plaintiffs and Class members had when that data was in the bank environment.

b. Plaid misappropriated Plaintiffs' and Class members' valuable banking data, sold it, and stored and used it for its own purposes.

**F. Violations of 18 U.S.C. § 1030(a)(6)**

293. Plaid knowingly trafficked in passwords or similar information through which a computer may be accessed without authorization under 18 U.S.C. §§ 1030(a)(6), 1030(e)(1), and 1029(e)(5) by knowingly obtaining control of access tokens or similar information from Plaintiffs' and Class members' financial institutions through which the institutions' computer systems could be accessed without authorization, with the intent to transfer such access tokens or



1 similar information to the Participating Apps so the Participating Apps could access Plaintiffs'  
 2 and Class members' private data from the institutions, including Plaintiffs' and Class members'  
 3 detailed banking transaction histories.

4 294. Alternatively, Plaid knowingly trafficked in passwords or similar information  
 5 through which a computer may be accessed without authorization under 18 U.S.C. §§ 1030(a)(6),  
 6 1030(e)(1), and 1029(e)(5) by knowingly transferring to the Participating Apps access tokens or  
 7 similar information from Plaintiffs' and Class members' banks through which the banks'  
 8 computer systems could be accessed without authorization using Plaid's software, so that those  
 9 entities so could use such access tokens or similar information to access Plaintiffs' and Class  
 10 members' private data from the banks, including Plaintiffs' and Class members' detailed banking  
 11 transaction histories.

12 295. Plaid acted with intent to defraud in trafficking the above-described passwords or  
 13 similar information under 18 U.S.C. §§ 1030(a)(6) & 1029(e)(5) by obtaining control of access  
 14 tokens or similar information and transferring such access tokens or similar information to the  
 15 Participating Apps with the intent that those entities would use such access tokens or similar  
 16 information to collect banking data to which they were not entitled, and that Plaid would be able  
 17 to charge the Participating Apps for the information or access.

18 296. Plaid's trafficking activities affected interstate or foreign commerce under 18  
 19 U.S.C. § 1030(a)(6).

20 **G. Plaintiffs' Right to Recover Damages**

21 297. As alleged above, Plaintiffs and Class members have suffered damage or loss by  
 22 reason of Plaid's violations of the CFAA and are therefore entitled to recover compensatory  
 23 damages, as well as injunctive or other equitable relief as prayed for below, all pursuant to 18  
 24 U.S.C. § 1030(g). Plaid's conduct has caused Plaintiffs and Class members losses in an amount  
 25 exceeding \$5,000 during a one-year period as required under 18 U.S.C. §§ 1030(g) and  
 26 1030(c)(4)(i)(I).

27 298. Plaintiffs bring this cause of action within two years of the date of the discovery of  
 28 their damages under 18 U.S.C. § 1030(g).

**THIRD CAUSE OF ACTION**

**Violation of the Stored Communications Act (“SCA”), 18 U.S.C. § 2701**

299. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

300. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class (referred to in this claim as “the Class”).

301. The Stored Communications Act prohibits a person from intentionally accessing without (or in excess of) authorization a facility through which an electronic communications service is provided and thereby obtaining an electronic communication while it is in “electronic storage.”

302. Each financial institution linked or verified for use with an Participating App, or each such institution’s systems and servers, is a facility, which provides its users with the ability to send and receive electronic communications, including, *inter alia*, images, data, queries, messages, notifications, statements, forms, updates, and intelligence regarding the financial institutions and their policies and promotions, as well as about customers’ individual accounts and activities, among others. 18 U.S.C. §§ 2701(a)(1); 2711(1), 2510(15) & 2510(12). Financial institutions communicate information about account holders’ financial affairs, including *inter alia* account balances, historical transactions, pending transactions, withdrawals, deposits, transfers, outgoing wires, loan terms, and interest rates through the electronic interface provided by financial institutions for access via web browsers and the institutions’ mobile apps.

303. The SCA defines “electronic storage” as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” Plaintiffs’ and Class members’ financial institution store the communications alleged herein in their respective systems and databases and on their respective servers.

1           304. For purposes of this cause of action only, the communications at issue exclude any  
2 electronic funds transfer information stored by a financial institution in a communications system  
3 used for the electronic storage and transfer of funds.

4           305. The communications at issue in this cause of action were in electronic storage  
5 within the meaning of 18 U.S.C. § 2510(17) in that they were stored, among other reasons, for  
6 purposes of backup protection of such electronic communications. Financial institutions  
7 necessarily store historical communications regarding a customer's past banking activities,  
8 historical direct messages, and other communications so that they may be accessed by consumers,  
9 including Plaintiffs and Class members (*e.g.*, for tax purposes, to confirm that an authorized  
10 payment was delivered, or to check on the status of a check).

11           306. Plaid's conduct in accessing these facilities and the communications stored  
12 thereon, was intentional.

13           307. Plaid violated 18 U.S.C. § 2701(a)(1) when it intentionally accessed Plaintiffs' and  
14 Class members' financial institutions and their systems and databases without authorization, and  
15 thereby obtained access to the contents of Plaintiffs' and Class members' electronic  
16 communications while those communications were in electronic storage on such systems. Plaid's  
17 access to the banks' computer systems was not authorized by Plaintiffs or the financial  
18 institutions.

19           308. Plaid's access to these facilities was achieved through subterfuge. Insofar as Plaid  
20 obtained purported authorization for its conduct, Plaid exceeded any such authorization by  
21 collecting, aggregating, selling, and divulging the contents of Plaintiffs' and Class members'  
22 electronic banking communications that were unrelated to the purpose for which Plaintiffs used  
23 the Participating Apps. 18 U.S.C. § 2701(a)(2). Plaid acquired communications far in excess of  
24 any information necessary to the Participating Apps for which account verification and linking  
25 were undertaken.

26           309. Plaintiffs and Class members are aggrieved by, and suffered concrete and  
27 particularized injury resulting from, Plaid's acquisition of their communications from financial  
28

1 institutions because they suffered economic, privacy, and human dignity harms as a result, as  
 2 alleged herein, including without limitation at ¶¶ 102-29.

3 310. As persons aggrieved by Plaid's knowing and intentional violations of the SCA,  
 4 Plaintiffs and Class members are entitled to appropriate relief under 18 U.S.C. § 2707, including  
 5 (i) preliminary and other equitable or declaratory relief as prayed for below, (ii) damages, and  
 6 (iii) reasonable attorneys' fees and costs.

7 311. For damages, Plaintiffs and Class members are entitled to recover their actual  
 8 damages, as well as all profits made by Plaid as a result of their violations. In addition, because  
 9 Plaid's violations of the SCA were willful or intentional, Plaintiffs and Class members also are  
 10 entitled to punitive damages.

11 312. Plaintiffs and Class members bring this cause of action within two years after the  
 12 date upon which they first discovered or had a reasonable opportunity to discover Plaid's  
 13 violations under 18 U.S.C. § 2707(f).

#### 14 **FOURTH CAUSE OF ACTION**

##### 15 **Declaratory Judgment that Plaid Wrongfully Accessed, Collected, Stored, Disclosed, Sold,** 16 **and Otherwise Improperly Used Plaintiffs' Private Data and Injunctive Relief**

17 313. Plaintiffs incorporate the substantive allegations contained in all prior and  
 18 succeeding paragraphs as if fully set forth herein.

19 314. Plaintiffs bring this claim on behalf of the Nationwide Class (referred to in this  
 20 claim as "the Class").

21 315. The gravamen of this controversy lies in Plaid's failure to inform consumers of its  
 22 true nature and conduct, and Plaid's subsequent invasions of their privacy. Plaintiffs and Class  
 23 members never consented to sharing their bank login credentials with Plaid, never agreed to share  
 24 their private, personal banking history and data with Plaid, never assented to Plaid gathering,  
 25 storing, disclosing, selling, or otherwise using their private, personal data.

26 316. Plaid's misconduct has put Plaintiffs' and Class members' financial privacy and  
 27 security at risk, and violated their dignitary rights, privacy, and economic well-being.

1 Accordingly, Plaintiffs seek appropriate declaratory relief, and injunctive relief as prayed for  
2 below.

### 3 **FIFTH CAUSE OF ACTION**

#### 4 **Unjust Enrichment (Quasi-Contract Claim for Restitution and Disgorgement)**

5 317. Plaintiffs incorporate the substantive allegations contained in all prior and  
6 succeeding paragraphs as if fully set forth herein.

7 318. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class  
8 (referred to in this claim as “the Class”).

9 319. Plaid has unjustly received benefits at the expense of Plaintiffs and the Class.

10 320. Plaid acquired and compromised the security of troves of private, personal banking  
11 records and transaction data that rightfully belong to Plaintiffs and the Class without informing  
12 them of these risks and through intentionally deceptive practices conducted in connection with  
13 consumers’ use of the Participating Apps.

14 321. The unethical, unfair, and deceptive practices Plaid employed to acquire and  
15 compromise this information include, without limitation: mimicking bank interfaces to cause  
16 Plaintiffs and Class members reasonably to believe they were providing their login credentials to  
17 their financial institutions, rather than a third party company; disguising Plaid’s appearance in the  
18 Participating Apps such that Plaintiffs and Class members were not made aware of the presence  
19 and conduct of a third party application; failing to correct material misleading information  
20 provided by Plaid’s fintech clients to Plaintiffs and Class members, such as that their credentials  
21 would “never be made accessible” to the Participating Apps and that their credentials were  
22 “Secure”; and concealing that Plaid collects all available banking data from all available accounts  
23 after it has accessed a consumer’s original, primary account.

24 322. Plaid was enriched when it utilized fraudulently obtained financial institution login  
25 credentials to access, collect, store, aggregate, use, and sell—to the Participating Apps—years’  
26 worth of Plaintiffs’ and Class members’ private banking records and transaction data. Plaid has  
27 derived profits and other tangible benefits from this collection of data, without which Plaid could  
28 not have grown its business, sold its platform to various and multiple developers, and developed

1 other apps. Furthermore, Plaid has directly and substantially profited from its use, storage,  
2 aggregation, and sale of Plaintiffs' and Class members' data.

3 323. In exchange for these benefits to Plaid, Plaintiffs and Class members received  
4 nothing. In fact, Plaintiffs and Class members were impoverished because, in order to benefit its  
5 bottom line, Plaid sacrificed Plaintiffs' and Class members' financial security and privacy, and  
6 violated their dignitary rights by perpetrating its deception.

7 324. Plaintiffs and Class members have suffered actual harm, including the increased  
8 risk of the loss or theft of their financial data and the dignitary harms inherent in the intrusion of  
9 personal privacy.

10 325. Plaintiffs and the Class seek an order that Plaid disgorge the profits and other  
11 benefits it has unjustly obtained.

## 12 **SIXTH CAUSE OF ACTION**

### 13 **Violation of Cal. Bus. & Prof. Code § 17200 *et seq.***

14 326. Plaintiffs incorporate the substantive allegations contained in all prior and  
15 succeeding paragraphs as if fully set forth herein.

16 327. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class  
17 (referred to in this claim as "the Class").

18 328. California law applies to the Class here because California has significant contacts,  
19 or significant aggregation of contacts, to the claims of each Class member, including that Plaid is  
20 a California company with its headquarters in California, and conducts substantial business in  
21 California. Additionally, the scheme described herein originated in California and the conduct  
22 alleged herein emanated from California. And, upon information and belief, Class members' data  
23 is pulled, stored, and aggregated by Plaid in California.

24 329. Plaid's conduct as alleged herein constitutes unfair, unlawful, or fraudulent  
25 business acts or practices as prohibited by California's Unfair Competition Law, Cal. Bus. &  
26 Prof. Code § 17200, *et seq.* (the "UCL").

1           **A.       “Unlawful” Prong of the UCL**

2           330.   Plaid’s conduct is “unlawful” under the UCL. Plaid violated the Computer Fraud  
3 and Abuse Act, 18 U.S.C. § 1030; the Stored Communications Act, 18 U.S.C. § 2701;  
4 California’s Comprehensive Data Access and Fraud Act, Cal. Pen. Code § 502; California’s Anti-  
5 Phishing Act of 2005, Cal. Bus. & Prof. Code § 22948.2; CalFIPA, Cal. Fin. Code § 4051, *et*  
6 *seq.*; CalOPPA, Cal. Bus. & Prof. Code § 22575, *et seq.*; the GLBA’s Privacy Rule, 16 C.F.R.  
7 Part 313, and Reg. P, 12 C.F.R. Part 1016; Cal. Civ. Code § 1709; and Article 1, § 1 of the  
8 California Constitution.

9           **B.       “Unfair” Prong of the UCL**

10          331.   Plaid’s conduct also is “unfair” under the UCL. California has a strong public  
11 policy of protecting consumers’ privacy interests, including protecting consumers’ banking data.  
12 Plaid violated this public policy by, among other things, surreptitiously collecting Plaintiffs’ and  
13 Class members’ private bank login information, using that login information to access their bank  
14 accounts, accessing and copying Plaintiffs’ and Class members’ private banking data, selling and  
15 transferring that data to Venmo and other fintech clients, and storing and using that data for its  
16 own purposes, all without Plaintiffs’ and Class members’ consent.

17          332.   Plaid’s conduct also violated the important public interests protected by the  
18 Computer Fraud and Abuse Act, 18 U.S.C. § 1030; the Stored Communications Act, 18 U.S.C.  
19 § 2701; California’s Comprehensive Data Access and Fraud Act, Cal. Pen. Code § 502;  
20 California’s Anti-Phishing Act of 2005, Cal. Bus. & Prof. Code § 22948.2; CalFIPA, Cal. Fin.  
21 Code § 4051, *et seq.*; CalOPPA, Cal. Bus. & Prof. Code § 22575, *et seq.*; the GLBA’s Privacy  
22 Rule, 16 C.F.R. Part 313, and Reg. P, 12 C.F.R. Part 1016; Cal. Civ. Code § 1709; and Article 1,  
23 § 1 of the California Constitution.

24          333.   Plaintiffs and Class members did not anticipate and could not have anticipated this  
25 degree of intrusion into their privacy. Plaid’s conduct did not create a benefit that outweighs these  
26 strong public policy interests. Rather, Plaid’s conducts narrowly benefitted Plaid and its fintech  
27 clients at the expense of the privacy of tens of millions of people. In addition, the effects of  
28 Plaid’s conduct were comparable to or substantially the same as the conduct forbidden by the

1 California Constitution and the common law's prohibitions against invasion of privacy, in that  
2 Plaid's conduct invaded fundamental privacy interests.

3 **C. "Fraudulent" Prong of the UCL**

4 334. Plaid's conduct is "fraudulent" under the UCL. Plaid makes a practice of spoofing  
5 bank websites in the software it incorporates into the Participating Apps for the purpose of  
6 surreptitiously collecting consumers' private bank login information, without the consumers'  
7 knowledge or consent. Plaid also makes a practice of using consumers' private bank login  
8 information to access their bank accounts, accessing and copying Plaintiffs' and Class members'  
9 private banking data, selling and transferring that data to the Participating Apps, and storing and  
10 using that data for its own purposes, all without the consumers' knowledge or consent. These  
11 business practices are likely to deceive members of the public and, indeed, have accomplished  
12 widespread public deception.

13 **D. Plaintiffs' Injuries and Rights to Relief**

14 335. Plaintiffs and Class members suffered injury in fact and lost money and /or  
15 property as the result of Plaid's unfair, unlawful, and fraudulent business practices, including  
16 when:

17 a. Plaid removed Plaintiffs' and Class members' banking data from the secure  
18 banking environment, selling or transferring it to the Participating Apps and storing it for Plaid's  
19 own use. Plaid thereby (1) destroyed the valuable indemnification rights Plaintiffs and Class  
20 members had against loss when that data was in the banking environment; and (2) removed  
21 valuable additional protections (including regulatory protections) Plaintiffs and Class members  
22 had when that data was in the banking environment.

23 b. Plaid misappropriated Plaintiffs' and Class members' property in the form of their  
24 exclusive records of their banking activities, sold it, and stored and used it for its own purposes.

25 336. As a result of Plaid's violations of the UCL, Plaintiffs and Class members are  
26 entitled to restitution, disgorgement by Plaid of the wrongfully-obtained private data obtained  
27 from their financial accounts, including without limitation a return of that data to Plaintiffs and  
28



1 Class members and the Plaintiffs' and Class members' financial institutions with corresponding  
 2 protections and security, and injunctive relief as prayed for below.

3 337. Section 17203 of the UCL authorizes a court to issue injunctive relief "as may be  
 4 necessary to prevent the use or employment by any person of any practice which constitutes  
 5 unfair competition." Plaintiffs and Class members seek injunctive relief as prayed for below.

## 6 **SEVENTH CAUSE OF ACTION**

### 7 **Violation of Article I, Section I of the California Constitution**

8 338. Plaintiffs incorporate the substantive allegations contained in all prior and  
 9 succeeding paragraphs as if fully set forth herein.

10 339. Plaintiffs James Cottle, David Evans, Logan Mitchell, Frederick Schoeneman,  
 11 Gabriel Sotelo, and Jeffrey Umali bring this claim on behalf of themselves and the California  
 12 Class.

13 340. The California Constitution expressly provides for and protects the right to privacy  
 14 of California citizens: "All people are by nature free and independent and have inalienable rights.  
 15 Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting  
 16 property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const., art. I, § 1.

17 341. Plaintiffs and California Class members have a reasonable expectation of privacy  
 18 in their confidential financial affairs, including without limitation in the personal information and  
 19 banking data maintained at their financial institutions. Plaintiffs and California Class members  
 20 reasonably expected that their login credentials, account numbers, balances, transaction history,  
 21 and other information was private and secure within the institutions at which they maintain  
 22 accounts. They reasonably expected that their information and data (a) would be protected and  
 23 secured against access by unauthorized parties; (b) would not be obtained by unauthorized  
 24 parties; (c) would not be transmitted or stored outside of the secure bank environment; and  
 25 (d) would not be sold or used without their knowledge or permission.

26 342. Plaintiffs and California Class members have a legally protected privacy interest in  
 27 preventing the unauthorized access, dissemination, sale, and misuse of their sensitive and  
 28 confidential banking information and data.

1           343. Plaid intentionally violated Plaintiffs’ and California Class members’ privacy  
2 interests. Plaid intruded upon Plaintiffs’ and California Class members’ sensitive and confidential  
3 banking information in a manner sufficiently serious in nature, scope, and actual or potential  
4 impact to constitute an egregious breach of the social norms underlying the privacy right.

5           344. Plaid intentionally violated Plaintiffs’ and California Class members’ privacy  
6 interests by improperly accessing, downloading, transferring, selling, storing and using their  
7 private banking information and data.

8           345. Plaid’s violations of Plaintiffs’ and California Class members’ privacy interests  
9 would be highly offensive to a reasonable person, especially considering (a) the highly sensitive  
10 and personal nature of Plaintiffs’ and California Class members’ banking information and data;  
11 (b) the extensive scope of data obtained by Plaid, including years of historical transactional data;  
12 (c) Plaid’s intent to profit from Plaintiffs’ and California Class members’ data by selling it  
13 outright and using it to develop further products and services; and (d) the fact that Plaid used  
14 subterfuge to intrude into Plaintiffs’ and California Class members’ banks’ secure environment  
15 for the purpose of collecting their data. Plaid’s intrusions were substantial and constituted an  
16 egregious breach of social norms.

17           346. Plaintiffs and California Class members did not consent to Plaid’s violations of  
18 their privacy interests.

19           347. Plaintiffs and California Class members suffered actual and concrete injury as a  
20 result of Plaid’s violations of their privacy interests. Plaintiffs and California Class members are  
21 entitled to appropriate relief, including damages to compensate them for the harm to their privacy  
22 interests, loss of valuable rights and protections, heightened risk of future invasions of privacy,  
23 and the mental and emotional distress and harm to human dignity interests caused by Plaid’s  
24 invasions, as well as disgorgement of profits made by Plaid as a result of its violations of their  
25 privacy interests.

26           348. Plaintiffs and California Class members also seek punitive damages because  
27 Plaid’s actions—which were malicious, oppressive, and willful—were calculated to injure  
28 Plaintiffs and California Class members and made in conscious disregard of Plaintiffs’ and

1 California Class members' rights. Punitive damages are warranted to deter Plaid from engaging in  
2 future misconduct.

### 3 **EIGHTH CAUSE OF ACTION**

#### 4 **Violation of Anti-Phishing Act of 2005, Cal. Bus. & Prof. Code § 22948 *et seq.***

5 349. Plaintiffs incorporate the substantive allegations contained in all prior and  
6 succeeding paragraphs as if fully set forth herein.

7 350. Plaintiffs James Cottle, David Evans, Logan Mitchell, Frederick Schoeneman,  
8 Gabriel Sotelo, and Jeffrey Umali bring this claim on behalf of themselves and the California  
9 Class.

10 351. The California Anti-Phishing Act of 2005 ("CAPA"), Cal. Bus. & Prof. Code  
11 § 22948.2 prohibits deceptive procurement of personal information that can be used to access the  
12 financial accounts of California residents. CAPA provides that it is "unlawful for any person, by  
13 means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit,  
14 request, or take any action to induce another person to provide identifying information by  
15 representing itself to be a business without the authority or approval of the business." CAPA, Cal.  
16 Bus. & Prof. Code § 22948.1, defines "identifying information" to include, *inter alia*, bank  
17 account numbers, account passwords, and any other piece of information that can be used to  
18 access an individual's financial accounts.

19 352. Plaid acquired identifying information in the form of Plaintiffs' and California  
20 Class members' bank account usernames and password information, codes received through the  
21 financial institutions' two-factor authentication processes, and all other identifying information  
22 sufficient for Plaid to access Plaintiffs' and California Class members' financial accounts.

23 353. Plaid obtained this identifying information in violation of Cal. Bus. & Prof. Code  
24 § 22948.2 by engaging in a pattern and practice of deception over several years (from no later  
25 than 2016 to present) affecting tens or hundreds of millions of consumers, including Plaintiffs and  
26 California Class members, namely, by designing and presenting consumer-facing interfaces in  
27 which to enter financial account usernames and passwords to appear as though they originated  
28 from financial institutions rather than a third-party data aggregator, without obtaining the

1 authority or approval of each financial institution. Plaid successfully designed the interfaces to  
2 mimic the login websites of financial institutions by using the banks' logos and color schemes, by  
3 presenting each interface in the context of verifying ownership of a financial account, by  
4 presenting each interface in a fashion that mirrored the experience of standard OAuth procedures  
5 wherein consumers *are* communicating in a secure manner with their financial institutions, and  
6 by failing to provide warnings and disclosures that a reasonable consumer would expect to  
7 receive when their financial institution login credentials are requested by any party *other* than  
8 their own financial institution. Each of these unlawful acts by Plaid was done without obtaining  
9 the authority or approval of each financial institution in order to cause Plaintiffs and California  
10 Class members to believe they were communicating with their financial institutions, and to thus  
11 to obtain Plaintiffs' and California Class members' identifying information. Through these  
12 means, Plaid did obtain Plaintiffs' and California Class members' bank login information.

13 354. Plaintiffs and California Class members have been adversely affected by Plaid's  
14 violation of Section 22948.2 because they are the direct and intended victims of Plaid's phishing.  
15 Each Plaintiff and California Class member provided their identifying information to Plaid under  
16 false pretenses and was injured because Plaid obtained that information by deceiving them.  
17 Plaintiffs and California Class members are also adversely affected by Plaid's conduct in using  
18 their identifying information, including without limitation because Plaid accessed the sensitive  
19 information stored in their financial accounts, and because Plaid used that information to acquire  
20 profits and other benefits for itself, unjustly under the circumstances, and at the expense of the  
21 security of Plaintiffs' and California Class members' financial information as compared to when  
22 the information was solely accessible to each individual account holder and their financial  
23 institution, as alleged herein.

24 355. Plaintiffs and California Class members are entitled to relief under Cal. Bus. &  
25 Prof. Code § 22948.3(a)(2), including the following:

26 a. Injunctive relief as prayed for below;  
27  
28

b. An order requiring Plaid to account for, hold in constructive trust, pay over to Plaintiffs and the California Class, and otherwise disgorge all profits derived by Plaid from its unlawful conduct and unjust enrichment, as permitted by law;

c. An award to Plaintiffs and the California Class of damages, including but not limited to, compensatory, statutory, treble, exemplary, aggravated, and punitive damages, as permitted by law and in such amounts to be proven at trial;

d. An award to Plaintiffs of reasonable costs, including reasonable attorneys' fees;

e. For pre-and post-judgment interest as allowed by law; and

f. For such other relief as the Court may deem just and proper.

### **NINTH CAUSE OF ACTION**

#### **Violation of Cal. Civ. Code §§ 1709 & 1710**

356. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

357. Plaintiffs James Cottle, David Evans, Logan Mitchell, Frederick Schoeneman, Gabriel Sotelo, and Jeffrey Umali bring this claim on behalf of themselves and the California Class.

358. California Civil Code § 1709 provides that “[o]ne who willfully deceives another with intend to induce him to alter his position to his injury or risk, is liable for any damage which he thereby suffers.”

359. California Civil Code § 1710 defines “deceit” as (1) the suggestion, as a fact, of that which is not true, by one who does not believe it to be true; (2) the assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true; (3) the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact; or (4) a promise, made without any intention of performing it.

360. Throughout the class period, Plaid engaged in deceit by intentionally concealing and failing to disclose its true nature and conduct to consumers. Plaid knew that representations made within the Participating Apps were misleading and material, and that the facts Plaid failed

1 to disclose and concealed were material. Plaid owed a duty to Plaintiffs and the California Class  
2 to provide them material information about its acquisition and use of their financial account  
3 credentials, including without limitation about the extent, duration, and consistency of Plaid's  
4 collection of private data from their financial accounts. Plaid's omissions and nondisclosures  
5 described herein were likely to deceive reasonable consumers, and have deceived Plaintiffs and  
6 the California Class. Plaid's acts of deceit include without limitation the following:

7 a. Plaid designed the software incorporated into the Participating Apps so that it  
8 would deceive consumers as to the existence of Plaid as a separate entity, Plaid's status as a third  
9 party, and the nature of Plaid's role as a data aggregator. Plaid suppresses these facts while under  
10 a duty to disclose them.

11 b. In Plaid's software incorporated in the Participating Apps, Plaid makes multiple  
12 statements that are misleading and give rise to a duty to disclose the true state of affairs to  
13 consumers. In the Venmo and Coinbase apps, for example (as in every Participating App  
14 utilizing the template forms designed by Plaid), one such statement promises that the system is  
15 "private," and that the consumer's "credentials will never be made accessible" to Venmo or  
16 Coinbase. Plaid makes this statement while knowing that the system is designed not to be private  
17 because it involves passing credentials to Plaid as a third-party data aggregator, and involves the  
18 acquisition by third parties of the consumer's most private banking data. By stating that the login  
19 credentials will not be made accessible to Venmo or Coinbase, consumers are falsely led to  
20 believe that their credentials are not shared outside of the bank they know and trust, while Plaid  
21 in fact knows those credentials are intercepted by Plaid for its use in connecting to the bank.  
22 Another misleading statement in the Plaid software incorporated in the Venmo and Coinbase  
23 apps promises that the system is "Secure," and that the consumer's information is "encrypted  
24 end-to-end." In fact, Plaid knows that the system is designed not to be secure, including because  
25 (1) Plaid uses it to collect, sell, use, and store consumers' most private financial data; (2) Plaid  
26 fails to exercise control or oversight over how that data is stored or used after it sells it to its  
27 clients; and (3) when Plaid removes consumer banking data from the secure banking  
28 environment, it thereby destroys valuable protections afforded to consumers in the event of data

1 breach/theft. And by stating that the consumer's information is encrypted end-to-end, consumers  
2 are falsely led to believe that no entity outside of each Participating App and the bank ever  
3 receives access to any consumer information. At the same time Plaid makes the foregoing  
4 statements, Plaid simultaneously suppresses the true facts while under a duty to disclose them.

5 c. In Plaid's software incorporated in the Participating Apps, Plaid makes a practice  
6 of spoofing bank login websites for the purpose of deceiving consumers into believing they are  
7 logging into their bank, when in fact they are passing their bank login information directly to  
8 Plaid. Plaid thereby suggests to consumers that they are entering their bank login information in  
9 a secure manner, when Plaid knows that is not true.

10 d. In its privacy policy, Plaid intentionally conceals and fails to disclose (1) the fact  
11 that Plaid collects consumer bank login information directly, (2) the fact that Plaid uses bank  
12 login information to access consumers' accounts, (3) the fact that Plaid collects all available  
13 banking data from every available account once it accesses the original account; (4) the fact that  
14 Plaid sells the consumer banking data it collects to the Participating Apps; (5) the fact that Plaid  
15 does not exercise adequate oversight over how consumer banking data is stored or used after it  
16 sells that data to the Participating Apps; (6) the fact that Plaid otherwise uses and monetizes the  
17 consumer banking data it collects; (7) the fact that Plaid stores the consumer banking data it  
18 collects; (8) the fact that the Participating Apps purchase, use, and store the consumer banking  
19 data collected by Plaid; (9) the fact that Plaid continues to access accounts and collect, sell and  
20 use consumer banking data long after the initial connection is made, regardless of whether the  
21 consumer uses the Participating Apps; and (10) the fact that, by removing consumer banking  
22 data from the secure banking environment, Plaid is destroying valuable indemnification rights  
23 afforded to consumers. Plaid suppresses those facts while under a duty to disclose them.

24 e. Plaid falsely states in its privacy policy that the information it receives from banks  
25 "varies depending on the specific Plaid services developers use to power their applications." In  
26 fact, Plaid knows that it collects all available consumer banking information when it connects  
27 with a consumer's bank, regardless of the services the Participating Apps choose to use.  
28

f. By stating in the Plaid privacy policy that Plaid collects “[i]nformation about account transactions, including amount, date, payee, type, quantity, price, location, involved securities, and a description of the transaction,” Plaid intentionally deceives consumers who use the Participating Apps into believing that Plaid only collects information about transactions conducted using the Participating Apps. Plaid thereby suppresses the fact that it collects years’ worth of transactions entirely unrelated to the consumer’s use of the Participating Apps, while giving information of other facts which are likely to mislead for want of communication of that fact.

361. Plaid’s omissions and nondisclosures were pervasive. Plaintiffs and the California Class members have reasonably relied on the material omissions and nondisclosures made by Plaid.

362. Plaid’s misconduct alleged herein was intentional, deliberate, and willful, and was perpetrated with the intent to, *inter alia*, cause Plaintiffs and the California Class members unknowingly to divulge confidential login credentials that could be and were used by Plaid to access and collect private information stored within their financial accounts. Plaid thereby willfully deceived Plaintiffs and California Class members with the intent to induce them to alter their position to their injury or risk under Cal. Civ. Code § 1709.

363. Plaintiffs seek recovery of their and the California Class members’ resulting damages, including economic damages, restitution, and disgorgement, as well as punitive damages.

#### **TENTH CAUSE OF ACTION**

##### **Violation of California’s Comprehensive Data Access and Fraud Act, Pen. Code § 502**

364. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

365. Plaintiffs James Cottle, David Evans, Logan Mitchell, Frederick Schoeneman, Gabriel Sotelo, and Jeffrey Umali bring this claim on behalf of themselves and the California Class.



1           366. The California Legislature enacted the California Computer Data Access and  
2 Fraud Act, Cal. Penal Code § 502 (“CDAFA”), to “expand the degree of protection afforded to  
3 individuals . . . from tampering, interference, damage, and unauthorized access to (including the  
4 extraction of data from) lawfully created computer data and computer systems,” finding and  
5 declaring that “the proliferation of computer technology has resulted in a concomitant  
6 proliferation of . . . forms of unauthorized access to computers, computer systems, and computer  
7 data,” and that “protection of the integrity of all types and forms of lawfully created computers,  
8 computer systems, and computer data is vital to the protection of the privacy of individuals as  
9 well as to the well-being of financial institutions . . . .” Cal. Penal Code § 502(a).

10           367. There is no justification for Plaid’s undisclosed, but deliberate, misuse of  
11 Plaintiffs’ and California Class members’ mobile devices and computers, and of their financial  
12 institutions’ computers, to acquire their financial data. Plaintiffs and California Class members  
13 did not give express or implied permission to Plaid to take, alter, copy, and/or use data concerning  
14 their financial accounts as alleged herein.

15           368. Plaintiffs’ mobile devices, *e.g.*, their smartphones, constitute “computers,  
16 computer systems, and/or computer networks” within the meaning of the CDAFA. Plaintiffs’  
17 financial institutions use “computers, computer systems, and/or computer networks” within the  
18 meaning of the CDAFA to store financial information about Plaintiffs.

19           369. Plaid violated California Penal Code § 502(c)(1) by knowingly accessing and  
20 without permission damaging and using both Plaintiffs’ and California Class members’ financial  
21 institutions’ computer systems and their data contained therein, in order to (i) execute Plaid’s  
22 scheme to defraud and deceive by wrongfully collecting, selling and using Plaintiffs’ and  
23 California Class members’ private data, and (ii) wrongfully obtain money, as well as Plaintiffs’  
24 and California Class members’ valuable property and data.

25           370. Plaid violated California Penal Code § 502(c)(2) by knowingly accessing and  
26 without permission taking, copying, and making use of Plaintiffs’ and California Class members’  
27 private data from Plaintiffs’ and California Class members’ financial institutions’ computers,  
28 computer systems, or computer networks.

1           371. Plaid violated California Penal Code § 502(c)(3) by knowingly and without  
2 permission causing to be used Plaintiffs' and California Class members' financial institutions'  
3 computer services.

4           372. Plaid violated California Penal Code § 502(c)(4) by knowingly accessing and  
5 without permission damaging the integrity of Plaintiffs' and California Class members' financial  
6 institutions' computer systems, as well as Plaintiffs' and California Class members' data  
7 contained therein.

8           373. Plaid violated California Penal Code § 502(c)(6) by knowingly and without  
9 permission providing a means for the Participating Apps to access Plaintiffs' and California Class  
10 members' financial institutions' computer systems in violation of Penal Code Section 502 by  
11 using its software to surreptitiously collect Plaintiffs' and California Class members' bank login  
12 information, using it to establish connections to Plaintiffs' and California Class members' banks,  
13 and then selling access tokens to the Participating Apps so they could access and download  
14 Plaintiffs' and California Class members' private banking data.

15           374. Plaid violated California Penal Code § 502(c)(7) by knowingly and without  
16 permission accessing Plaintiffs' and California Class members' banks' computer systems.

17           375. Plaid violated California Penal Code § 502(c)(8) by knowingly introducing a  
18 computer contaminant into Plaintiffs' and California Class members' smartphones, in the form of  
19 the software it incorporated into the apps of the Participating Apps, to surreptitiously collect  
20 Plaintiffs' and California Class members' financial institution login information.

21           376. None of Plaintiffs, California Class members, nor Plaintiffs' and California Class  
22 members' financial institutions gave express or implied permission to Plaid to access their  
23 financial institutions' computer systems or the data stored therein. Plaintiffs and California Class  
24 members did not give express or implied permission to Plaid to access their smartphones.

25           377. Plaid accessed Plaintiffs' and California Class members' private banking data,  
26 Plaintiffs' and California Class members' banks' computer systems, and Plaintiffs' and California  
27 Class members' smartphones in a manner that circumvented technical or code-based barriers in  
28 place to restrict or bar third-party access.

378. As the owners of the private data that is the subject of this cause of action and persons who suffered damage or loss by reason of Plaid's above violations, Plaintiffs and California Class members are entitled under California Penal Code § 502(e) to pursue an action against Plaid for compensatory damages and injunctive relief or other equitable relief, including without limitation restitution of the revenue and other benefits accruing to Plaid by virtue of its violations of the CDAFA, as well as to recover reasonable attorneys' fees. And because Plaid's violations were willful and Plaid is guilty of oppression, fraud, or malice, Plaintiffs and California Class members also are entitled to an award of punitive or exemplary damages.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs request that judgment be entered against Plaid and that the Court grant the following:

A. An order determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are Class Representatives, that Plaintiffs' attorneys shall be appointed as Class Counsel pursuant to Rule 23(g) of the Federal Rules of Civil Procedure, and that Class notice be promptly issued;

B. Judgment against Plaid for Plaintiffs' and Class members' asserted claims for relief;

C. Appropriate declaratory relief against Plaid;

D. Equitable and injunctive relief requiring Plaid to: (1) purge the data it has unlawfully collected; (2) plainly and conspicuously disclose, on the first screen of its Plaid Link software, if and when presented to consumers, (a) that Plaid is a third party data aggregator providing connection services to consumers' financial institutions for the purpose of collecting private data from their financial institutions, (b) that it is not necessary for consumers to connect to their banks using Plaid; and (c) that using Plaid's services will eliminate consumers' indemnification rights provided by financial institutions; (3) obtain, before it connects with a consumer's financial account, affirmative permission from the consumer for each action Plaid takes in connection with the account, including accessing, copying, selling, storing, and using data; (4) before it connects with a consumer's financial account, require the consumer to review

the full text of Plaid's privacy policy, acknowledge all of the terms and conditions by checking boxes to indicate their consent to those provisions, and acknowledge receipt and approval of the notice; (5) obtain a consumer's affirmative consent each time Plaid accesses that consumer's financial account and financial data; and (6) notify consumers of Plaid's actions to remedy its unlawful conduct alleged herein, and steps consumers can take to prevent future and additional privacy invasions by Plaid and other actors to whom Plaid has sold or otherwise delivered their personal information;

E. Equitable and injunctive relief enjoining Plaid from: (1) accessing, attempting to access, or procuring transmission of any California Class member's identifying information through their financial accounts; (2) representing that any solicitation, request, or action by Plaid is being done by a financial institution; (3) retaining any copies, electronic or otherwise, of any identifying information obtained through the phishing scheme alleged herein; (4) retaining any copies, electronic or otherwise, of any other information obtained from any of Plaintiffs' or California Class members' financial institutions using identifying information obtained through the phishing scheme alleged herein; and (5) engaging in any unlawful activities alleged herein;

F. An order awarding Plaintiffs and the Class members actual and/or statutory and/or special and/or incidental damages as well as restitution;

G. An order requiring Plaid to pay punitive damages, dignitary damages, and exemplary damages;

H. An order requiring Plaid to pay pre-judgment and post-judgment interest;

I. Reasonable attorney's fees and costs reasonably incurred; and

J. Any and all other and further relief to which Plaintiffs and the Classes may be entitled.

//

### **DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand a trial by jury of all issues so triable.

1 Dated: August 5, 2020

HERRERA PURDY LLP

2 By: /s/ Shawn Kennedy

3 Shawn M. Kennedy

4 Shawn M. Kennedy (SBN 218472)

skennedy@herrerapurdy.com

5 Andrew M. Purdy (SBN 261912)

apurdy@herrerapurdy.com

6 Bret D. Hembd (SBN 272826)

bhembd@herrerapurdy.com

7 4590 MacArthur Blvd., Suite 500

8 Newport Beach, CA 92660

9 Tel: (949) 936-0900

Fax: (855) 969-2050

10 HERRERA PURDY LLP

11 Nicomedes Sy Herrera (SBN 275332)

nherrera@herrerapurdy.com

12 Laura E. Seidl (SBN 269891)

lseidl@herrerapurdy.com

13 1300 Clay Street, Suite 600

14 Oakland, California 94612

Tel: (510) 422-4700

15 Fax: (855) 969-2050

16 Dated: August 5, 2020

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

17 By: /s/ Rachel Geman

18 Rachel Geman

19 Rachel Geman (*Pro Hac Vice*)

20 rgeman@lchb.com

21 250 Hudson Street, 8th Floor

New York, NY 10013-1413

22 Tel: (212) 355-9500

23 Fax: (212) 355-9592

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP  
Michael W. Sobol (SBN 194857)  
msobol@lchb.com  
Melissa Gardner (SBN 289096)  
mgardner@lchb.com  
275 Battery Street, 29th Floor  
San Francisco, CA 94111-3339  
Tel: (415) 956-1000  
Fax: (415) 956-1008

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP  
Madeline M. Gomez (*Pro Hac Vice*)  
mgomez@lchb.com  
222 2nd Avenue South, Suite 1640  
Nashville, TN 37201  
Tel: (615) 313-9000  
Fax: (212) 313-9965

Dated: August 5, 2020

BURNS CHAREST LLP

By: /s/ Christopher Cormier  
Christopher J. Cormier

Christopher J. Cormier (*Pro Hac Vice*)  
ccormier@burnscharest.com  
4725 Wisconsin Avenue, NW, Suite 200  
Washington, DC 20016  
Tel: (202) 577-3977  
Fax: (469) 444-5002

BURNS CHAREST LLP  
Warren T. Burns (*Pro Hac Vice*)  
wburns@burnscharest.com  
Russell Herman (*Pro Hac Vice*)  
rherman@burnscharest.com  
900 Jackson Street, Suite 500  
Dallas, TX 75202  
Tel: (469) 904-4550  
Fax: (469) 444-5002

1 BURNS CHAREST LLP  
2 C. Jacob Gower (*Pro Hac Vice*)  
3 jgower@burnscharest.com  
4 365 Canal Street, Suite 1170  
5 New Orleans LA 70130  
6 Tel: (504) 799-2845  
7 Fax: (504) 881-1765

*Interim Co-Lead Class Counsel*

8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
NUSSBAUM LAW GROUP, P.C.

Linda P. Nussbaum (*Pro Hac Vice*)  
lnussbaum@nussbaumpc.com  
Bart D. Cohen (*Pro Hac Vice* to be Filed)  
bcohen@nussbaumpc.com  
1211 Avenue of the Americas, 40th Floor  
New York, NY 10036  
Tel: (917) 438-9102  
Fax: (212) 753-0396

REINHARDT WENDORF & BLANCHFIELD

Garrett D. Blanchfield  
g.blanchfield@rwblawfirm.com  
Roberta A. Yard  
r.yard@rwblawfirm.com  
Mark Reinhardt  
m.reinhardt@rwblawfirm.com  
(*Pro Hac Vice* Applications forthcoming)  
332 Minnesota Street, Suite W-105  
St. Paul, MN 55101  
Tel: (651) 287-2100  
Fax: (651) 287-2103

ROBINS KAPLAN LLP

Aaron M. Sheanin (SBN 214472)  
asheanin@robinskaplan.com  
2440 W El Camino Real, Suite 100  
Mountain View, CA 94040  
Tel: (650) 784-4040

ROBINS KAPLAN LLP

Kellie Lerner (*Pro Hac Vice* to be filed)  
klerner@robinskaplan.com  
Hollis Salzman (*Pro Hac Vice* to be filed)  
hsalzman@robinskaplan.com  
William Reiss (*Pro Hac Vice* to be filed)  
wreiss@robinskaplan.com  
Benjamin Steinberg (*Pro Hac Vice* to be filed)  
BSteinberg@RobinsKaplan.com  
Matthew J. Geyer (*Pro Hac Vice*)  
MGeyer@robinskaplan.com  
399 Park Avenue, Suite 3600  
New York, NY 10022  
Tel: (212) 980-7400

SPECTOR ROSEMAN & KODROFF, P.C.

William G. Caldes  
BCaldes@srkattorneys.com  
Jeffery L. Spector  
JSpector@srkattorneys.com  
Jeffrey L. Kodroff  
JKodroff@srkattorneys.com  
Diana J. Zinser  
DZinser@srkattorneys.com  
(*Pro Hac Vice* Applications forthcoming)  
2001 Market Street, Suite 3420  
Philadelphia, PA 19103  
Tel: (215) 496-0300  
Fax: (215) 496-6611

*Interim Plaintiffs' Steering Committee*